Security in-a-box provides the knowledge you need to recognise digital security threats and the tools you need to address them. It offers detailed, step-by-step instructions to help you use those tools effectively, as well as practical, non-technical advice for anyone who relies on digital technology to do sensitive advocacy work.

www.tacticaltech.org
www.frontlinedefenders.org

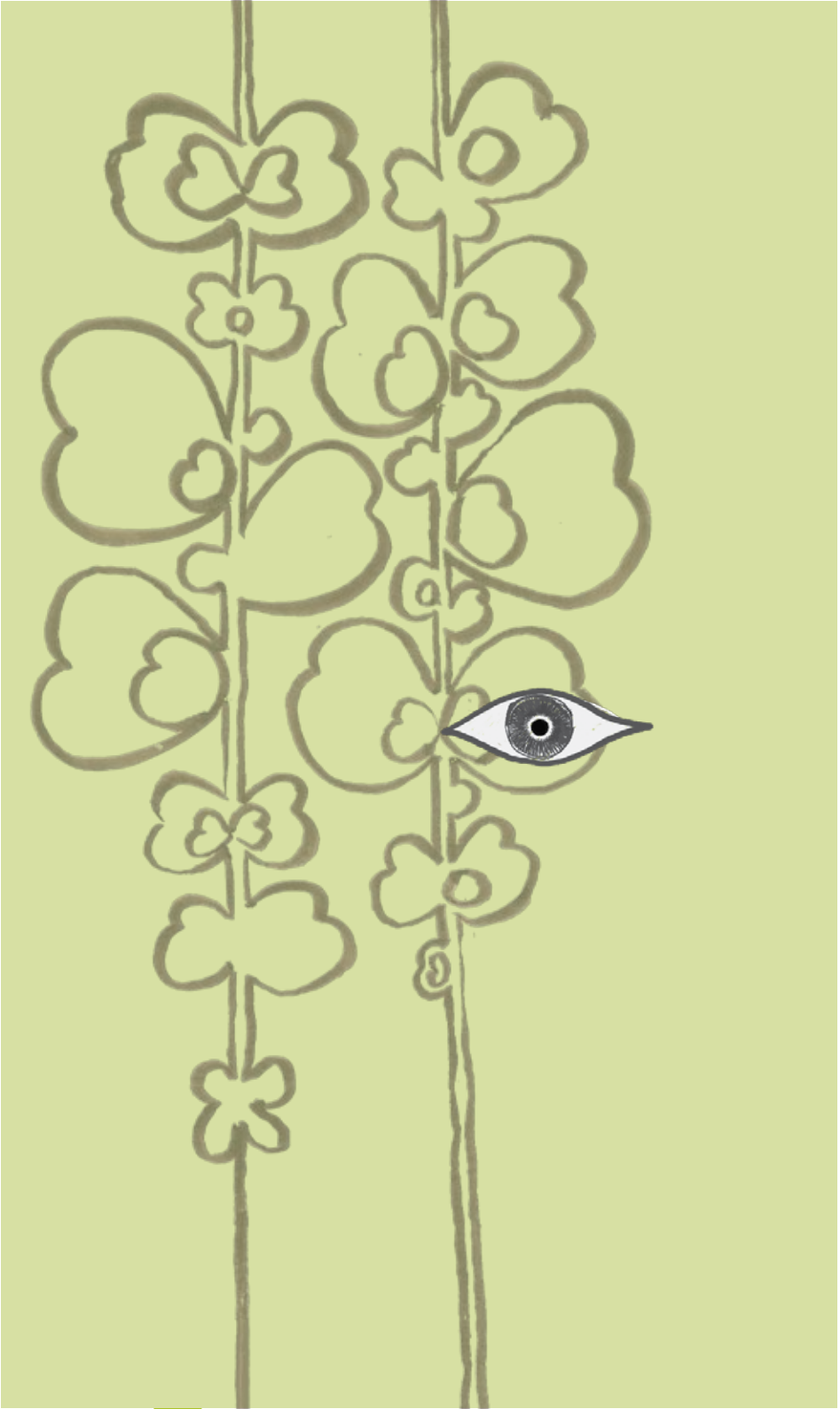
TACTICAL TECHNOLOGY COLLECTIVE

Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

TOOLS AND TACTICS FOR ADVOCACY

security in-a-box

tools and tactics for your digital security



security in-a-box

tools and tactics for your digital security

TOOLS AND TACTICS FOR ADVOCACY

Security in-a-box was developed by the
Tactical Technology Collective and Front Line in collaboration with:

Coordination, writing & editing	Wojtek Bogusz Dmitri Vitaliev Chris Walker
Additional writing	Cormac McGuire Benji Pereira
English proofreading & copy editing	Caroline Kraabel Benji Pereira
Lead tester	Rosemary Warner
Design	Lynne Stuart
Curriculum development	Pamela Teitelbaum Dmitri Vitaliev
Coordination of software localisation	Louise Berthilson Alberto Escudero Pascual
Spanish team	
Translation	Phol Edward Paucar Aguirre
Editing	Katitza Rodríguez Pereda
Webmaster	Angelin Venegas Ramírez
Localisation	Diego Escalante Urrelo
Proofreading	Carlos Wertheman
French Team	
Editing, translation & localisation	Patrick Cadorette
Translation & localisation	Alexandre Guédon
Proofreading	Miriam Heap-Lalonde
Editing	Fabian Rodriguez
Russian Team	
Translation	Emin Akhundov
Translation	Alexei Bebinov
Translation	Alexander Lapidus
Proofreading	Ksenia Shiryaeva
Editing, translation & localisation	Sergei Smirnov
Arabic Team	
Editing, translation & localisation	Ahmad Gharbeia
Editing	Manal Hassan
Translation & localisation	Khaled Hosny
Translation	Mahammad F Kalfat
Special Thanks to	The Citizen Lab, Robert Guerra, Internews, RiseUp,The Tor Project & VaultletSoft
Funder	

TABLE OF CONTENTS

Introduction 1

1. How to protect your computer from malware and hackers 9
Viruses 10
Spyware 12
Firewalls 13
Keeping your software up-to-date 15

2. How to protect your information from physical threats 21
Assessing your risks 21
Protecting your information from physical intruders 23
Maintaining a healthy environment for your computer hardware 26
Creating your physical security policy 27

3. How to create and maintain secure passwords 33
Selecting and maintaining secure passwords 33
Remembering and recording secure passwords 35

4. How to protect the sensitive files on your computer 43
Encrypting your information 44
Hiding your sensitive information 46

5. How to recover from information loss 53
Identifying and organising your information 54
Defining your backup strategy 56
Creating a digital backup 58
Recovering from accidental file deletion 61

6. How to destroy sensitive information 67
Deleting information 68
Wiping information with secure deletion tooll 69
Tips on using secure deletion tools effectively 71
Tips on wiping the entire contents of a storage device 72

7. How to keep your Internet communication private 77
Securing your email 78
Tips on responding to suspected email surveillance 83
Securing other Internet communication tools 84
Advanced email security 85

8. How to remain anonymous and bypass censorship on the Internet 93
Understanding Internet censorship 94
Understanding censorship circumvention 96
Anonymity networks and basic proxy servers 97
Specific circumvention proxies 101

Glossary 107

Introduction

Advocates are increasingly concerned about their digital security, and with good reason. While computers and the Internet can be extremely powerful tools for advocacy, they also expose groups (that may already be quite vulnerable) to new risks. As more advocates have begun to rely on digital technology to achieve their outreach, data-collection, information design, communication and mobilisation objectives, these risks have become greater.

If you are an advocate who focuses on sensitive issues, or you work closely with such people, then you have probably experienced (or heard stories about) digital security and privacy threats. Computers and backup drives that were confiscated, passwords that changed mysteriously, local websites that were hacked or overloaded by malicious Internet traffic, foreign websites that can no longer be accessed and emails that appear to have been forged, blocked, modified or read by someone other than the intended recipient. These are true stories, and many of them are set in an environment that makes matters even worse, one in which computer operating systems are frequently out-of-date, software is often pirated and viruses run rampant.

This toolkit provides explanations of, and solutions for, threats like these. It was created by a diverse team of experts who understand not only the conditions under which advocates work, but also the resource restrictions they face.

While ***Security in-a-box*** is designed primarily to address the growing needs of advocates in the global South, particularly human rights defenders, the software and strategies in this toolkit are relevant to digital security in general. It has something to offer anyone who works with sensitive information. This may include vulnerable minorities and independent journalists or 'whistle-blowers', in addition to advocates working on a range of issues, from environmental justice to anti-corruption campaigns.

HOW TO USE THE SECURITY IN-A-BOX TOOLKIT

This toolkit has three major components:

- the ***How-to Booklet***
- the ***Hands-on Guide***
- a selection of freeware and Open Source software

This ***How-to Booklet*** is designed to explain the issues that you must understand in order to safeguard your own digital security. It seeks to identify and describe the risks you face and help you make informed

decisions about how best to reduce those risks. To this end, it answers eight broad questions related to basic security, data protection and communication privacy.

At the beginning of each chapter, you will find a ***background scenario*** populated by fictional characters who will reappear in brief conversations throughout the chapter in order to illustrate certain points and answer common questions. You will also find a short list showing ***what you can learn from this chapter***. It is a good idea to scan through this list before you begin reading. As you work through a chapter, you will encounter a number of technical terms that are highlighted in green and defined in the glossary at the end of the booklet. You will also find references to the specific software discussed in the toolkit's ***Hands-on Guides***.

These ***Hands-on Guides*** are included, along with an electronic copy of the ***How-to Booklet***, on the accompanying CD (or USB memory stick, if you have a version of the toolkit that contains one). Each guide explains how to use a particular freeware or Open Source software tool. The ***Hands-on Guides*** highlight potential difficulties, suggest helpful tips and, most importantly, walk you through the process of configuring and using these tools securely. They include screenshots and step-by-step instructions for you to follow as you go along.

All of this software can be installed directly from the toolkit or downloaded free of charge from the Internet. In most cases, you can install a tool simply by clicking on the appropriate link at the beginning of whichever guide explains that tool, then telling your browser to Open or Run the install program. If a Hands-on Guide provides special installation instructions, you may have to save a file to your Desktop, or some other location, in order to install that tool. The ***Security in-a-box*** disc also includes a section called ***Portable Security***, where you will find 'portable' versions of a few ***Security in-a-box*** tools. These versions are meant to be installed directly onto a USB memory stick so that you can use them on any computer.

Any single chapter or guide in this toolkit can be read individually, or formatted in your browser for easy printing, or shared electronically. However, you will get more out of ***Security in-a-box*** if you can follow the relevant links and references that are scattered throughout both the booklet and the software guides. Ideally, you will have this booklet in front of you while you work through the ***Hands-on Guides***. You should also remember to finish reading the ***How-to Booklet*** chapter covering a particular tool before you begin relying on that tool to protect your digital security.

Where possible, you should read the chapters of this booklet in order. Security is a process, and there is often little point in trying to defend yourself against an advanced threat to your communication privacy, for example, if you have not yet ensured that your computer is free of viruses and other malware. In many cases, this would be like locking your door after a burglar is already in your home. This is not to say that any one of these eight topics is more important than any other, it is simply that the later chapters make certain assumptions about what you already know and about the state of the computer on which you are about to install software.

Of course, there are many good reasons why you might want to work through these chapters out of sequence. You might need advice on how to back up your important files before you begin installing the tools described in the first ***Hands-on Guide***. You might find yourself faced with an urgent privacy threat that justifies learning ***How to protect the sensitive files on your computer***, which is covered in Chapter 4, as quickly as possible. Perhaps you are working from an Internet café, on a computer whose security is not your responsibility and from which you do not intend to access any sensitive information. If you want to use this computer to visit a website that is blocked in your country, there is nothing to prevent you from skipping ahead to ***Chapter 8: How to remain anonymous and bypass censorship on the Internet***.

Whatever path you take through the toolkit, we hope it answers some of your questions, helps you understand some of your vulnerabilities and shows you where to look for solutions.

ABOUT THE SECURITY IN-A-BOX PROJECT

Digital security and privacy threats are always unique to the work that an advocate does and the environment in which that person operates. Furthermore, the collection of software that might help address those threats is constantly changing, and the tools themselves are frequently updated. For these reasons, it is extremely difficult to create an 'off-the-shelf' toolkit like Security in-a-box. Nothing stated in this toolkit is absolute, and there is no replacement for a trusted, local expert who understands the environment you work in, is sympathetic to your cause and can help you identify the most up-to-date tools with which to protect yourself.

Nevertheless, we hope that ***Security in-a-box*** will give you an idea of the relevant issues and the right solutions for your own particular situation. We have worked with experts from all over the globe to peer-review the tools and tactics that make up this toolkit. This booklet offers the very best advice that we could assemble without being able to look at and respond to your unique circumstances.

The software that we selected was researched, tested and, in many cases, localised into additional languages by a diverse team of security experts, advocates, human rights defenders, translators and software engineers in collaboration with the Tactical Technology Collective and Front Line. These tools featured prominently in a number of security trainings that were held as part of the ***Security in-a-box*** project, trainings that served not only to strengthen the security and privacy of advocates throughout the world, but also to confirm the appropriateness of the tools selected and to verify the accuracy of the ***Hands-on Guides***.

As of this booklet's publication, the entire toolkit is available in five languages: English, Arabic, French, Russian and Spanish. It exists both as a printed toolkit, and on the ***Security in-a-box*** website, at ***www.security.ngoinabox.org.*** Please write to ***security@ngoinabox.org*** if you would like to request additional copies, distribute or translate the toolkit or talk to us about training.

Tactical Tech and Front Line are dedicated to making this toolkit as useful as possible for advocates, and to ensuring that future versions are even better. To do so, we rely heavily on your feedback. Your stories about the toolkit – how you use it, what you find useful and what you don't find useful – will help us get it right. They will also help us raise funds for the further development of this project. Please send us your comments, stories and ideas to ***security@ngoinabox.org***.

1
How to protect your computer from malware and hackers

1. How to protect your computer from malware and hackers

Regardless of your broader objectives, keeping your computer healthy is a critical first step down the path toward better security. So, before you begin worrying too much about strong passwords, private communication and secure deletion, for example, you need to make sure that your computer is not vulnerable to **hackers** or plagued by malicious software, often called **malware**, such as viruses and spyware. Otherwise, it is impossible to guarantee the effectiveness of any other security precautions you might take. After all, there is no in point locking your door if the burglar is already downstairs, and it doesn't do you much good to search downstairs if you leave the door wide open.

Accordingly, this chapter explains how to maintain your software and use tools like **Avast**, **Spybot** and **Comodo Firewall** to protect your computer against the ever-present dangers of malware infection and **hacker** attacks. Although the tools recommended in this chapter are for Windows, which is the operating system most vulnerable to these threats, **GNU/Linux** and Apple OS X users are also at risk and should still adopt the tactics presented below.

Background scenario

Assani is a human rights activist in a Francophone African country. His two teenage children, Salima and Muhindo, have offered to help him with some routine computer work he has been asked to do. After seeing the state of his computer, they offer to teach him the basics of how to keep it healthy and functional. Assani also likes the idea of using Free and Open Source Software, but he's not sure whether that would be more or less secure, so he asks for their advice.

What you can learn from this chapter

- More about the nature of a few of the specific threats that **malware** poses to the privacy and integrity of your information, the stability of your computer and the reliability of other security tools
- How you can use a number of recommended tools to help protect yourself from these threats
- How to keep your computer secure by updating your software frequently
- Why you should use **freeware** tools, to avoid the dangers associated with expired licenses or pirated software, and popular **FOSS** tools, where possible, to enhance your security.

VIRUSES

There are many different ways to classify viruses, and each of these methods comes with its own set of colorfully-named categories. Worms, macroviruses, trojans and backdoors are some of the more well-known examples. Many of these viruses spread over the Internet, using email, malicious webpages or other means to infect unprotected computers. Others spread through removable media, particularly devices like USB memory sticks and external hard drives that allow users to write information as well as reading it. Viruses can destroy, damage or infect the information in your computer, including data on external drives. They can also take control of your computer and use it to attack other computers. Fortunately there are many anti-virus tools that you can use to protect yourself and those with whom you exchange digital information.

Anti-virus software

There is an excellent **freeware** anti-virus program for Windows called **Avast**, which is easy to use, regularly updated and well-respected by anti-virus experts. It requires that you register once every 14 months, but registration, updates and the program itself are all free-of-charge.

Hands-on: Get started with the *Avast Guide*

Clam Win is a **FOSS** alternative to Avast and the various well-known commercial anti-virus programs. Although it lacks certain features that are important for a primary anti-virus program, Clam Win has the advantage that it can be run from a USB memory stick in order to scan a computer on which you are not allowed to install software. This is extremely helpful when you have no choice but to use public computers or Internet cafes for sensitive work.

Tips on using anti-virus software effectively

- Do not run two anti-virus programs at the same time, as this might cause your computer to run extremely slowly or to crash. Uninstall one before installing another.
- Make sure that your anti-virus program allows you to receive updates. Many commercial tools that come pre-installed on new computers must be registered (and paid for) at some point or they will stop receiving updates. All of the software recommended here supports free updating.
- Ensure that your anti-virus software updates itself regularly. New viruses are written and distributed every day, and your computer will quickly become vulnerable if you do not keep up with new virus definitions. Avast will automatically look for updates when you are connected to the Internet.
- Enable your anti-virus software's 'always on' virus-detection feature if it has one. Different tools have different names for it, but most of them offer a feature like this. It may be called 'Realtime Protection,' 'Resident Protection,' or something similar. Take a look at *Section 3.2.1* of the *Avast Guide* to learn more about that tool's 'Resident Scanner.'
- Scan all of the files on your computer regularly. You don't have to do this every day (especially if your anti-virus software has an 'always on' feature, as described above) but you should do it from time to time. How often may depend on the circumstances. Have you connected your computer to unknown networks recently? With whom have you been sharing USB memory sticks? Do you frequently receive strange attachments by email? Has someone else in your home or office recently had virus problems? For more information on how best to scan files, see the *Avast Guide*.

Preventing virus infection

- Be extremely cautious when opening email attachments. It is best to avoid opening any attachment received from an unknown source. If you need to do so, you should first save the attachment to a folder on your computer, then open the appropriate application (such as Microsoft Word or Adobe Acrobat) yourself. If you use the program's File menu to open the attachment manually, rather than double-clicking the file or allowing your email program to open it automatically, you are less likely to contract a virus.
- Consider the possible risks before inserting removable media, such as CDs, DVDs and USB memory sticks, into your computer. You should first check that your anti-virus program has the latest updates and that its scanner is running. It is also a good idea to disable your operating system's 'AutoPlay' feature, which can be used by viruses to infect your computer. Under Windows XP, this can be done by going inside My Computer, right-clicking on your CD or DVD drive, selecting Properties and clicking on the AutoPlay tab. For each content type, select the Take no action or Prompt me each time to choose an action options then click OK.
- You can also help prevent some virus infections by switching to free and open source software, which is often more secure, and which virus writers are less likely to target.

Assani: *I have a virus cleaner and I run it regularly, so I figure my computer is healthy, right?*

Salima: *Actually, just having anti-virus software isn't enough. You also need to protect your computer from spyware and hackers, so you'll have to install and run a couple more tools.*

SPYWARE

Spyware is a class of malicious software that can track the work you do, both on your computer and on the Internet, and send information about it to someone who shouldn't have access to it. These programs can record the words you type on your keyboard, the movements of your mouse, the pages you visit and the programs you run, among other things. As a result, they can undermine your computer's security and reveal confidential information about you, your activities and your contacts. Computers become infected with spyware in much the same way that they contract viruses, so many of the suggestions above are also helpful when defending against this second class of malware. Because malicious webpages are a major source of spyware infection, you should pay extra attention to the websites you visit and make sure that your browser settings are secure.

Assani: *It all sounds like something out of a spy movie to me. Is my computer really "infected with spyware?"*

Muhindo: *Believe it or not, it's really common. If those programs you downloaded from the Internet haven't infected you, there's a good chance at least one of the webpages you've visited has. The fact that you use Windows and Internet Explorer makes it even more likely. If you've never scanned your computer for spyware, I bet you'll be surprised by how much is already installed on it*

Anti-spyware software

You can use anti-spyware tools to protect your computer from this type of threat. Spybot is one such program, and it does a very good job of identifying and removing certain types of malware that anti-virus programs simply ignore. Just like with anti-virus software, though, it is extremely important that you update Spybot's malware definitions and run regular scans.

Hands-on: Get started with the *Spybot Guide*

Preventing spyware infection

- Stay alert when browsing websites. Watch for browser windows that appear automatically, and read them carefully instead of just clicking Yes or OK. When in doubt, you should close 'pop up windows' by clicking the X in the upper right-hand corner, rather than by clicking Cancel. This can help prevent webpages from tricking you into installing malware on your computer.
- Improve the security of your Web browser by preventing it from automatically running the potentially dangerous programs that are sometimes contained within webpages you visit. If you are using Mozilla **Firefox**, you can install the **NoScript** add-on, as described in *Section 4* of the *Firefox Guide*.
- Never accept and run this sort of content if it comes from websites that you don't know or trust.

Assani: *I've heard that 'Java applets' and 'ActiveX controls' can be dangerous. But I have no idea what they are.*

Salima: *They're just different examples of the same sort of thing: small programs that your Web browser sometimes downloads along with whatever page you're reading. Web designers use them to create complex sites, but they can also spread viruses and spyware. You don't have to worry too much about how they actually work, as long as you have NoScript installed and running properly.*

FIREWALLS

A firewall is the first program on a computer that sees incoming data from the Internet. It is also the last program to handle outgoing information. Like a security guard, posted at the door of a building to decide who can enter and who can leave, a firewall receives, inspects and makes decisions about all incoming and outgoing data. Naturally, it is critical that you defend yourself against untrusted connections from the Internet and from local networks, either of which could give hackers and viruses a clear path to your computer. In fact, though, monitoring outgoing connections originating from your own computer is no less important.

A good firewall allows you to choose access permissions for each program on your computer. When one of these programs tries to contact the outside world, your firewall will block the attempt and give you a warning unless it recognizes the program and verifies that you have given it permission to make that sort of connection. This is largely to prevent existing malware from spreading viruses or inviting hackers

into your computer. In this regard, a firewall provides both a second line of defense and an early-warning system that might help you recognize when your computer's security is being threatened.

Firewall software

Recent versions of Microsoft Windows include a built-in firewall, which is now turned on automatically. Unfortunately, the Windows firewall is limited in many ways. In particular, it does not examine outgoing connections, and it can be somewhat difficult to use. However, there is an excellent **freeware** program called **Comodo Firewall,** which does a better job of keeping your computer secure.

Hands-on: Get started with the *Comodo Firewall Guide*

Asani: *So, now you want me to install anti-virus, anti-spyware and firewall software? Can my computer cope with all that?*

Muhindo: *Absolutely. In fact, these three tools are the bare minimum if you want to stay secure on the Internet these days. They're made to work together, so installing them all shouldn't cause any problems. Remember, though, you don't want want to run two anti-virus programs or two firewalls at the same time.*

Preventing untrusted network connections

- Only install essential programs on the computer you use for sensitive work, and make sure you get them from a reputable source. Uninstall any software that you do not use.
- Disconnect your computer from the Internet when you are not using it and shut it down completely overnight
- Do not share your Windows password with anyone.
- If you have enabled any 'Windows services' that you are no longer using, you should disable them. See the *Further reading* section for more
- Make sure that all of the computers on your office network have a firewall installed
- If you do not already have one, you should consider installing an additional firewall to protect the entire local network at your office. Many commercial broadband **gateways** include an easy-to-use firewall, and turning it on can make your network much more secure. If you are not sure where to start with this, you might want to ask for assistance from whoever helped set up your network

KEEPING YOUR SOFTWARE UP-TO-DATE

Computer programs are often large and complex. It is inevitable that some of the software you use on a regular basis contains undiscovered errors, and it is likely that some of these errors could undermine your computer's security. Software developers continue to find these errors, however, and release updates to fix them. It is therefore essential that you frequently update all of the software on your computer, including the operating system. If Windows is not updating itself automatically, you can configure it to do so by clicking the **Start** menu, selecting **All Programs** and clicking **Windows Update**. This will open Internet Explorer, and take you to the Microsoft Update page, where you can enable the **Automatic Updates** feature. See the *Further reading* section to learn more about this.

Staying up-to-date with freeware and FOSS tools

Proprietary software often requires proof that it was purchased legally before it will allow you to install updates. If you are using a pirated copy of Microsoft Windows, for example, it may be unable to update itself, which would leave you and your information extremely vulnerable. By not having a valid license, you put yourself and others at risk. Relying on illegal software can present non-technical risks, as well. The authorities in a growing number of countries have begun to verify that organisations possess a valid license for each piece of software that they use. Police have confiscated computers and closed down organizations on the basis of 'software piracy.' This justification can be abused quite easily in countries where the authorities have political reasons to interfere with a given organisation's work. Fortunately, you do not have to purchase expensive software to protect yourself from tactics like this.

We strongly recommend that you try out the **freeware** or **FOSS** alternatives to any propriety software that you currently use, especially those programs that are unlicensed. Freeware and FOSS tools are often written by volunteers and non-profit organisations who release them, and even update them, free of charge. FOSS tools, in particular, are generally considered to be more secure than **proprietary** ones, because they are developed in a transparent way that allows their **source code** to be examined by a diverse group of experts, any one of whom can identify problems and contribute solutions.

Many FOSS applications look like, and work almost the same way as, the proprietary software that they were written to replace. At the same time, you can use these programs alongside proprietary software, including the Windows operating system, without any problems. Even if your colleagues continue to use the commercial version of a particular

type of program, you can still exchange files and share information with them quite easily. In particular, you might consider replacing Internet Explorer, Outlook or Outlook Express and Microsoft Office with Firefox, Thunderbird and OpenOffice, respectively.

In fact, you could even move away from the Microsoft Windows operating system entirely, and try using a more secure FOSS alternative called **GNU/Linux**. The best way to find out if you're ready to make the switch is simply to give it a try. You can download a **LiveCD** version of Ubuntu **GNU/Linux**, burn it to a CD or DVD, put it in your computer and restart. When it's done loading, your computer will be running GNU/Linux, and you can decide what you think. Don't worry, none of this is permanent. When you're finished, simply shut down your computer and remove the Ubuntu LiveCD. The next time you start up, you'll be back in Windows, and all of you applications, settings and data will be just as you left them. In addition to the general security advantages of open-source software, Ubuntu has a free, easy-to-use update tool that will keep your operating system and much of your other software from becoming outdated and insecure.

FURTHER READING

- See the chapter on *Malicious Software and Spam* and the Appendix on *Internet Program Settings* in the *Digital Security and Privacy for Human Rights Defenders* [1] book.
- Keep up to-date with news about viruses on the *Virus Bulletin* [2] website.
- Learn how to *determine which 'Windows services' are unnecessary* [3] and *disable those you do not need* [4].
- Other toolkits from the Tactical Technology Collective (*TTC*) [5] can help you switch to using FOSS and Freeware tools for all of your software needs.

LINKS

[1] ***www.frontlinedefenders.org/manual/en/esecman***
[2] ***www.virusbtn.com***
[3] ***https://security.berkeley.edu/MinStds/Determining-Un-Services-Windows.html***
[4] ***www.marksanborn.net/howto/turn-off-unnecessary-windows-services***
[5] ***www.tacticaltech.org***

2
Protect your information from physical threats

2. How to protect your information from physical threats

No matter how much effort you have put into building a digital barrier around your computer, you could still wake up one morning to find that it, or a copy of the information on it, has been lost, stolen, or damaged by any number of unfortunate accidents or malicious acts. Anything from a power surge to an open window to a spilt cup of coffee might lead to a situation in which all of your data are lost and you are no longer able to use your computer. A careful risk assessment, a consistent effort to maintain a healthy computing environment and a written **security policy** can help avoid this type of diaster.

Background scenario

Shingai and Rudo are an elderly married couple with many years of experience helping the HIV-infected population of Zimbabwe maintain access to proper medication. They are applying for a grant to purchase new computers and network equipment for their office. Since they live in a region that is quite turbulent, in terms both of politics and of infrastructure, they and their potential funders want to ensure that their new hardware will be safe, not only from hackers and viruses, but also from confiscation, thunder-storms, electrical spikes and other such disasters. They ask Otto, a local computer technician, to help them devise a plan of action to strengthen the physical security of the computers and network hardware they plan to buy if their grant application is successful.

What you can learn from this chapter

- More about a few of the **physical threats** to your computer and to the information stored on it
- How best to secure computer equipment against some of these threats
- How to create a healthy operating environment for computers and network equipment
- What to consider when creating a security plan for the computers in your office

ASSESSING YOUR RISKS

Many organisations underestimate the importance of keeping their offices and their equipment physically secure. As a result, they often

lack a clear policy describing what measures they should take to protect computers and backup storage devices from theft, severe weather conditions, accidents, and other physical threats. The importance of such policies may seem obvious, but formulating them properly can be more complicated than it sounds. Many organisations, for example, have good quality locks on their office doors, and many even have secure windows; but if they do not pay attention to the number of keys that have been created, and who has copies of those keys, their sensitive information remains vulnerable.

Shingai: ***We want to put a brief summary of our security policy into this grant application, but we also need to make sure the policy itself is thorough. What should we include in it?***

Otto: ***I'm afraid I can't recommend a one-size-fits-all solution to the challenge of physical security. The specifics of a good policy almost always depend on a particular organisation's individual circumstances. Here's a piece of general advice, though: when you're trying to come up with a plan, you need to observe your work environment very carefully and think creatively about where your weak points might be and what you can do to strengthen them.***

When assessing the risks and vulnerabilities that you or your organisation face, you must evaluate several different levels at which your data may be threatened.

- Consider the communication channels you use and how you use them. Examples might include paper letters, faxes, landline phones, mobile phones, emails and **Skype** messages.
- Consider how you store important information. Computer hard drives, email and web servers, USB memory sticks, external USB hard drives, CDs and DVDs, mobile phones, printed paper and handwritten notes are all likely possibilities.
- Consider where these items are located, physically. They could be in the office, at home, in a trash bin out back or, increasingly, 'somewhere on the Internet.' In this last case, it might be quite challenging to to determine the particular piece of information's actual, physical location.

Keep in mind that the same piece of information might be vulnerable on many different levels. Just as you might rely on anti-virus software to protect the contents of a USB memory stick from malware, you must rely on a detailed physical security plan to protect the same information from theft, loss or destruction. While some security practices, such as having a good off-site backup policy, are helpful against both digital and physical threats, others are clearly more specific.

When you decide whether to carry your USB memory stick in your pocket or sealed in a plastic bag at the bottom of your luggage, you are making a decision about physical security, even though the information you are trying to protect is digital. As usual, the correct policy depends greatly on the situation. Are you walking across town or travelling across a border? Will somebody else be carrying your bag? Is it raining? These are the sorts of questions that you should consider when making decisions like this.

PROTECTING YOUR INFORMATION FROM PHYSICAL INTRUDERS

Malicious individuals seeking access to your sensitive information represent one important class of physical threat. It would be a mistake to assume that this is the only such threat to the security of your information, but it would be even move shortsighted to ignore it. There are a number of steps you can take to help reduce the risk of physical intrusion. The categories and suggestions below, many of which may apply to your home as well as your office, represent a foundation upon which you should build in accordance with your own particular physical security situation.

Around the office

- Get to know your neighbours. Depending on the security climate in your country and in your neighbourhood, one of two things may be possible. Either you can turn them into allies who will help you keep an eye on your office, or you can add them to the list of potential threats that your security plan must address.
- Review how you protect all of the doors, windows and other points of entry that lead into your office.
- Consider installing a surveillance camera or a motion-sensor alarm.
- Try to create a reception area, where visitors can be met before they enter the office, and a meeting room that is separate from your normal work space.

In the office

- Protect network cables by running them inside the office.
- Lock network devices such as **servers**, **routers**, **switches**, **hubs** and modems into secure rooms or cabinets. An intruder with physical access to such equipment can install malware capable of stealing data in transit or attacking other computers on your network even after he leaves.

- If you have a wireless network, it is critical that you secure your **access point** so that intruders cannot join your network or monitor your traffic. If you are using an insecure wireless network, anyone in your neighbourhood with a laptop becomes a potential intruder. This is an unusual definition of 'physical', but it helps to consider that a malicious individual who can monitor your wireless network has the same access as one who can sneak into your office and connect an ethernet cable. The steps required to secure a wireless network will vary, depending on your access point hardware and software, but they are rarely difficult to follow.

At your work space

- You should position your computer screen carefully, both on your desk and when you are away from the office, in order to prevent others from reading what is displayed there. In the office, this means considering the location of windows, open doors and the guest waiting area, if you have one.
- Most desktop computer cases have a slot where you can attach a padlock that will prevent anyone without a key from getting inside. If you have cases like this in the office, you should lock them so that intruders cannot tamper with their internal hardware. You might also consider this feature when purchasing new computers.
- Use a locking **security cable**, where possible, to prevent intruders from stealing the computers themselves. This is especially important for laptops and small desktops that could be hidden inside a bag or under a coat.

Software and settings related to physical security

- Make sure that, when you restart your computer, it asks you for a password before allowing you to run software and access files. If it does not, you can enable this feature in Windows by clicking on the Start menu, selecting the Control Panel, and double-clicking on User Accounts. In the User Accounts screen, select your own account and click Create a Password. Choose a secure password, as discussed in *Chapter 3: How to create and maintain good passwords*, enter your password, confirm it, click Create Password and click Yes, Make Private.
- There are a few settings in your computer's **BIOS** that are relevant to physical security. First, you should configure your computer so that it will not **boot** from its floppy, CD-ROM or DVD drives. Second, you should set a password on the BIOS itself, so that an intruder can not simply undo the previous setting. Again, be sure to choose a secure password.
- If you rely on a secure password database, as discussed in *Chapter 3*, to store your Windows or BIOS passwords for a particular computer, make sure that you do not keep your only copy of the database on that computer.
- Get in the habit of locking your account whenever you step away from your computer. On Windows, you can do this quickly by holding down the Windows logo key and pressing the L key. This will only work if you have created a password for your account, as described above.
- **Encrypt** sensitive information on computers and storage devices in your office. See *Chapter 4: How to protect the sensitive files on your computer* for additional details and pointers to the appropriate Hands-on Guides.

Rudo: ***I'm a bit nervous about messing around in BIOS. Can I break my computer if I do something wrong?***

Otto: ***You sure can, at least for a little while. In fact, the settings that you might want to change are pretty simple, but the BIOS screen itself can be a little intimidating, and it is possible to leave your computer temporarily unable to start if you do something wrong. In general, if you're uncomfortable working in BIOS, you should ask someone with more computer experience to help you out.***

Portable devices

- Keep your laptop, your mobile phone and other portable devices that contain sensitive information with you at all times, especially if you are travelling or staying at a hotel. Travelling with a laptop **security cable** is a good idea, although it is sometimes difficult to find an appropriate object to which you can attach one. Remember that meal times are often exploited by thieves, many of whom have learnt to check hotel rooms for laptops during hours of the day when they are likely to be unattended.
- If you have a laptop, or a hand-held computing device such as a Personal Digital Assistant (PDA), try to avoid putting them on display. There is no need to show thieves that you are carrying such valuable hardware or to show individuals who might want access to your data that your shoulder bag contains a hard drive full of information. Avoid using your portable devices in public areas, and consider carrying your laptop in something that does not look like a laptop bag.

MAINTAINING A HEALTHY ENVIRONMENT FOR YOUR COMPUTER HARDWARE

Like many electronic devices, computers are quite sensitive. They do not adapt well to unstable electricity supplies, extreme temperatures, dust, high humidity or mechanical stress. There are a number of things you can do to protect your computers and network equipment from such threats:

- Electrical problems such as power surges, blackouts and brownouts can cause physical damage to a computer. Irregularities like this can 'crash' your hard drive, damaging the information it contains, or physically harm the electronic components in your computer.
  - If you can afford them, you should install Uninterruptible Power Supplies (**UPSs**) on important computers in your office. A UPS provides temporary power in the event of a blackout.
  - Even where UPSs are deemed inappropriate or too costly, you can still provide power filters or surge protectors, either of which will help protect you from power surges.
  - Test your electrical network before you connect important equip ment to it. Try to use power sockets that have three slots, one of them being a 'ground line', or 'earth'. And, if possible, take a day or two to see how the electrical system in a new office behaves when powering inexpensive devices, such as lamps and fans, before put ting your computers at risk.
- To defend against accidents in general, avoid placing important hardware in passages, reception areas or other easily accessible locations. UPSs, power filters, surge protectors, power strips and extension cables, particularly those attached to servers and networking equipment, should be positioned where they will not be switched off by an accidental misstep.
- If you have access to high-quality computer cables, power strips and extension cables, you should purchase enough to serve your entire office and pick up a few extras. Power strips that fall out of wall sockets, fail to hold plugs securely and spark constantly are more than just annoying. They can be quite damaging to the physical security of any computers attached to them. They can also lead frustrated users to secure their loose computer cables to a sparking power strip with tape, which creates an obvious fire hazard.
- If you keep any of your computers inside cabinets, make sure they have adequate ventilation, or they might overheat
- Computer equipment should not be housed near radiators, heating vents, air conditioners or other ductwork

Shingai: *Actually, we just solved a few of these problems earlier this year. We spent months trying to find cables that wouldn't fall out of the backs of our computers.*

Otto: *And power strips that didn't look like they were about to set the carpet on fire?*

Shingai: *That, too. In the end, Rudo had to bring some back from a trip to Johannesburg. Mind you, the electricity itself is still pretty unstable, but at least the equipment is easier to work with.*

CREATING YOUR PHYSICAL SECURITY POLICY

Once you have assessed the threats and vulnerabilities that you or your organisation face, you must consider what steps can be taken to improve your physical security. You should create a detailed **security policy** by putting these steps in writing. The resulting document will serve as a general guideline for yourself, your colleagues and any newcomers to your organisation. It should also provide a checklist of what actions should be taken in the event of various different physical security emergencies. Everybody involved should take the time to read, implement and keep up with these security standards. They should also be encouraged to ask questions and propose suggestions on how to improve the document.

Your physical security policy may contain various sections, depending on the circumstances:

- An office access policy that addresses the alarm systems, what keys exist and who has them, when guests are allowed in the office, who holds the cleaning contract and other such issues
- A policy on which parts of the office should be restricted to authorized visitors
- An inventory of your equipment, including serial numbers and physical descriptions
- A plan for securely disposing of paper rubbish that contains sensitive information
- Emergency procedures related to:
  - Who should be notified if sensitive information is disclosed or misplaced
  - Who to contact in the event of a fire, flood, or other natural disaster
  - How to perform certain key emergency repairs
  - How to contact the companies or organizations that provide services such as electrical power, water and Internet access
  - How to recover information from your off-site backup system. You

can find more detailed backup advice in *Chapter 5: How to recover from information loss*.

Your **security policy** should be reviewed periodically and modified to reflect any policy changes that have been made since its last review. And, of course, don't forget to back up your security policy document along with the rest of your important data. See the *Further reading* section for more information about creating a security policy.

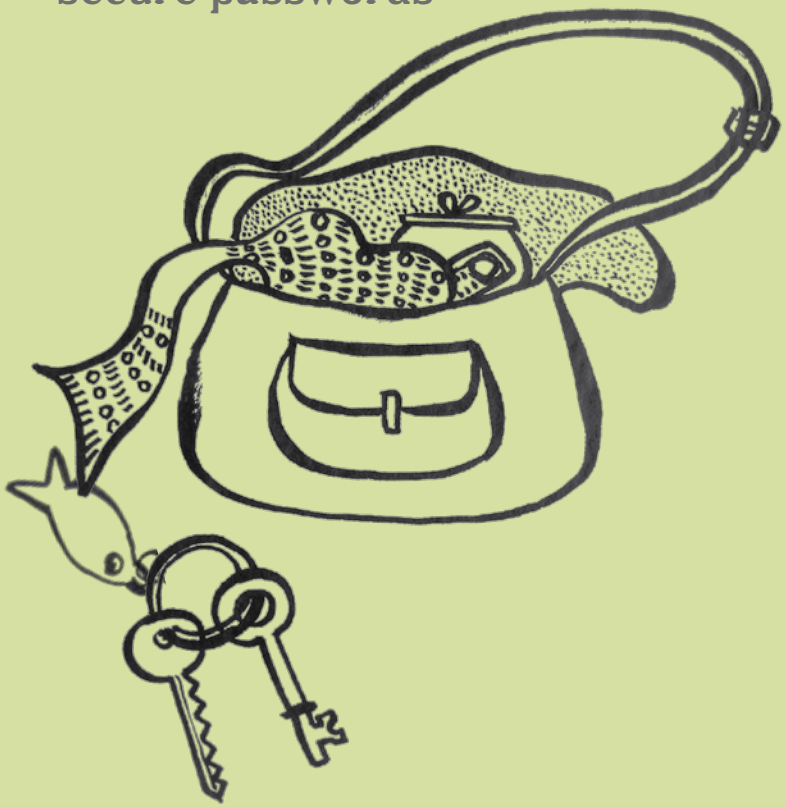
FURTHER READING

- For additional information on assessing risks, see the *Security Awareness*, and *Threat Assessment* sections of the *Digital Security and Privacy for Human Rights Defenders* book [1].
- For a more detailed explanation of how to set a BIOS password, see the *Windows Security* chapter in the *Digital Security and Privacy for Human Rights Defenders* book [1].
- For guidelines on creating a security policy, see *Case Study 1* in the *Digital Security and Privacy for Human Rights Defenders* book [1].
- See also the *Protection Manual* and *Protection Handbook* for Human Rights Defenders [1].

LINKS

[1] ***www.frontlinedefenders.org/manual/en/esecman***
[2] ***www.frontlinedefenders.org/manuals***

3
Create and maintain secure passwords



3. How to create and maintain secure passwords

Many of the secure services that allow us to feel comfortable using digital technology to conduct important business, from signing in to our computers and sending email to encrypting and hiding sensitive data, require that we remember a password. These secret words, phrases or strings of gibberish often provide the first, and sometimes the only, barrier between your information and anyone who might want to read, copy, modify or destroy it without your permission. There are many ways in which someone could learn your passwords, but you can defend against most of them by applying a few specific tactics and by using a secure password database tool, such as KeePass.

Background scenario

Mansour and Magda are siblings, in an Arabic-speaking country, who maintain a blog on which they anonymously publicise human rights abuses and campaign for political change. Magda recently tried to log into her personal webmail account and found that her password had been changed. After resetting the password, she was able to log in, but when she opened her inbox she noticed that several new messages were marked as having been read. She suspects that a politically-motivated intruder may have learned or guessed her password, which she uses for several of her website accounts. She is meeting with Mansour, who has less computer experience, to explain the situation and to voice her concerns.

What you can learn from this chapter

- The elements of a secure password
- A few tricks for remembering long, complicated passwords
- How to use the **KeePass secure password database** to store passwords instead of remembering them

SELECTING AND MAINTAINING SECURE PASSWORDS

In general, when you want to protect something, you lock it up with a key. Houses, cars and bicycle locks all have physical keys; protected files have **encryption** keys; bank cards have PIN numbers; and email accounts have passwords. All of these keys, physical and electronic, have one thing in common: they open their respective locks just as effectively in the hands of somebody else. You can install advanced firewalls, secure

email accounts, and **encrypted** disks, but if your password is weak, or if you allow it to fall into the wrong hands, they will not do you much good.

Elements of a strong password

A password should be difficult for a computer program to guess.

- **Make it long:** The longer a password is, the less likely it is that a computer program would be able to guess it in a reasonable amount of time. You should try to create passwords that include ten or more characters. Some people use passwords that contain more than one word, with or without spaces between them, which are often called passphrases. This is a great idea, as long as the program or service you are using allows you to choose long enough passwords.
- **Make it complex:** In addition to length, the complexity of a password also helps prevent automatic 'password cracking' software from guessing the right combination of characters. Where possible, you should always include upper case letters, lower case letters, numbers and symbols, such as punctuation marks, in your password.

A password should be difficult for others to figure out.

- **Make it practical:** If you have to write your password down because you can't remember it, you may end up facing a whole new category of threats that could leave you vulnerable to anybody with a clear view of your desk or temporary access to your home, your wallet, or even the trash bin outside your office. If you are unable to think of a password that is long and complex but still memorable, the *Remembering secure passwords* section, below, might be of some help. If not, you should still choose something secure, but you may need to record it using a **secure password database** such as **KeePass**. Other types of password-protected files, including Microsoft Word documents, should not be trusted for this purpose, as many of them can be broken in seconds using tools that are freely available on the Internet.
- **Don't make it personal:** Your password should not be related to you personally. Don't choose a word or phrase based on information such as your name, social security number, telephone number, child's name, pet's name, birth date, or anything else that a person could learn by doing a little research about you.
- **Keep it secret:** Do not share your password with anyone unless it is absolutely necessary. And, if you must share a password with a friend, family member or colleague, you should change it to a temporary password first, share that one, then change it back when they are done using it. Often, there are alternatives to sharing a password, such as creating a separate account for each individual who needs access. Keeping your password secret also means paying attention to who might be reading over your shoulder while you type it or look it up in a secure password database.

A password should be chosen so as to minimise damage if someone does learn it.

- **Make it unique:** Avoid using the same password for more than one account. Otherwise, anyone who learns that password will gain access to even more of your sensitive information. This is particularly true because some services make it relatively easy to crack a password. If you use the same password for your Windows user account and your Gmail account, for example, someone with physical access to your computer can crack the former and use what they learn to access the latter. For similar reasons, it is a bad idea to rotate passwords by swapping them around between different accounts.
- **Keep it fresh:** Change your password on a regular basis, preferably at least once every three months. Some people get quite attached to a particular password and never change it. This is a bad idea. The longer you keep one password, the more opportunity others have to figure it out. Also, if someone is able to use your stolen password to access your information and services without you knowing about it, they will continue to do so until you change the password.

Mansour: ***What if I trust someone? It's OK for me to tell you my password, right?***

Magda: ***Well, first of all, just because you trust somebody with your password doesn't necessarily mean you trust them to take good care of it, right? Even though I wouldn't do anything bad with your password, I might write it down and lose it or something. That could even be how I got into this mess! And besides, it's not all about trust. If you're the only one who knows your password, then you don't have to waste your time worrying about who to blame if the account gets broken into. Right now, for example, I feel pretty confident that somebody actually guessed or 'cracked' my password, because I never wrote it down or shared it with anyone.***

REMEMBERING AND RECORDING SECURE PASSWORDS

Looking over the list of suggestions above, you might wonder how anyone without a photographic memory could possibly keep track of passwords that are this long, complex and meaningless without writing

them down. The importance of using a different password for each account makes this even more difficult. There are a few tricks, however, that might help you create passwords that are easy to remember but extremely difficult to guess, even for a clever person using advanced 'password cracking' software.

You also have the option of recording your passwords using a tool like **KeePass** that was created specifically for this purpose.

Remembering secure passwords

It is important to use different types of characters when choosing a password. This can be done in various ways:

- Varying capitalisation, such as: 'My naME is Not MR. MarSter'
- Alternating numbers and letters, such as: 'a11 w0Rk 4nD N0 p14Y'
- Incorporating certain symbols, such as: 'c@t(heR1nthery3'
- Using multiple languages, such as: 'Let Them Eat 1e gateaU au ch() colaT'

Any of these methods can help you increase the complexity of an otherwise simple password, which may allow you to choose one that is secure without having to give up entirely on the idea of memorizing it. Some of the more common substitutions (such as the use of a zero instead of an 'o' or the '@' symbol in place of an 'a') were long-ago incorporated into password-cracking tools, but they are still a good idea. They increase the amount of time that such tools would require to learn a password and, in the more common situations where tools of this sort cannot be used, they help prevent lucky guesses.

Passwords can also take advantage of more traditional mnemonic devices, such as the use of acronyms. This allows long phrases to be turned into complex, seemingly-random words:

- 'To be or not to be? That is the question' becomes '2Bon2B?TitQ'
- 'We hold these truths to be self-evident: that all men are created equal' becomes 'WhtT2bs-e:taMac='
- 'Are you happy today?' becomes 'rU:-)2d@y?'

These are just a few examples to help you come up with your own method of encoding words and phrases to make them simultaneously complex and memorable.

Recording passwords securely

While a little creativity may allow you to remember all of your passwords, the need to change those passwords periodically means that you might quickly run out of creativity. As an alternative, you can generate random, secure passwords for most of your accounts and simply give up on the idea of remembering them all. Instead, you can record them in a portable, encrypted secure password database, such as KeePass.

Hands-on: Get started with the *KeePass Guide*

Of course, if you use this method, it becomes especially important that you create and remember a very secure password for **KeePass**, or whatever tool you choose. Whenever you need to enter a password for a specific account, you can look it up using only your master password, which makes it much easier to follow all of the suggestions above. KeePass is portable, as well, which means that you can put the database on a USB memory stick in case you need to look up a password while you are away from your primary computer.

Although it is probably the best option for anybody who has to maintain a large number of accounts, there are a few drawbacks to this method. First, if you lose or accidentally delete your only copy of a password database, you will no longer have access to any of the accounts for which it contained passwords. This makes it extremely important that you back up your KeePass database. Look over *Chapter 5: How to recover from information loss* for more information on backup strategies. Fortunately, the fact that your database is encrypted means that you don't have to panic if you lose a USB memory stick or a backup drive containing a copy of it.

The second major drawback could be even more important. If you forget your KeePass master password, there is no way to recover it or the contents of the database. So, be sure to choose a master password that is both secure and memorable!

Mansour: ***Wait a minute. If KeePass uses a single master password to protect all of your other passwords, how is it more secure than just using that same password for all of your accounts? I mean, if a bad guy learns the master password, he gets access to everything, right?***

Magda: ***It's a good thought, and you're right that protecting your master password is really important, but there are a couple of key differences. First of all, this 'bad guy' would not only need your password, he'd need your KeePass database file, too. If you just share the same password between all of your accounts, then he'd only need the password itself. Plus, we know that KeePass is extremely secure, right? Well, other programs and websites can go either way. Some of them are much less secure than others, and you don't want someone breaking into a weak***

website, and then using what he learns to access a more secure account. And there's another thing, too. KeePass makes it really easy to change your master password if you think it's necessary. I should be so lucky! I spent all day today updating my passwords.

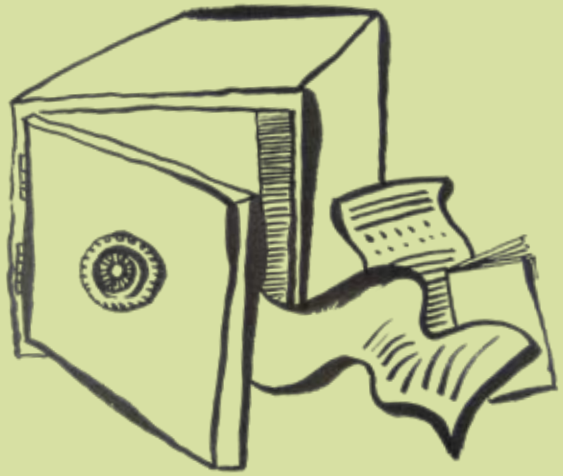
FURTHER READING

- To learn more about secure passwords, see the *Password Protection* chapter and the *How long should my password be?* Appendix in the *Digital Security and Privacy for Human Rights Defenders* book [1].
- Wikipedia has informative articles on *Passwords* [2], *Guidelines for password strength* [3], and *password cracking* [4].

LINKS

[1] ***www.frontlinedefenders.org/manual/en/esecman***
[2] ***www.en.wikipedia.org/wiki/Password***
[3]***www.en.wikipedia.org/wiki/Password_strength***
[4] ***www.en.wikipedia.org/wiki/Password_cracking***

4
Protect the sensitive files on your computer



4. How to protect the sensitive files on your computer

Unauthorised access to the information on your computer or portable storage devices can be carried out remotely, if the 'intruder' is able to read or modify your data over the Internet; or physically, if he manages to get hold of your hardware. You can protect yourself against either type of threat by improving the physical and network security of your data, as discussed in *Chapter 1: How to protect your computer from malware and hackers* and *Chapter 2: How to protect your information from physical threats*. It is always best to have several layers of defence, however, which is why you should also protect the files themselves. That way, your sensitive information is likely to remain safe even if your other security efforts prove inadequate.

There are two general approaches to the challenge of securing your data in this way. You can **encrypt** your files, making them unreadable to anyone but you, or you can hide them in the hope that an intruder will be unable to find your sensitive information. There are tools to help you with either approach, including a **FOSS** application called **TrueCrypt**, which can both encrypt and hide your file.

Background scenario

Claudia and Pablo work with a human rights NGO in a South American country. They have spent several months collecting testimonies from witnesses to the human rights violations that have been committed by the military in their region. If the details of who provided these testimonies were to become known, it would endanger both the courageous people who testified and members of the organisation in that region. This information is currently stored in a spreadsheet on the NGO's Windows XP computer, which is connected to the Internet. Being security conscious, Claudia has made sure to store a backup of the data on a CD, which she keeps outside the office.

What you can learn from this chapter

- How to encrypt information on your computer
- What risks you might face by keeping your data encrypted
- How to protect data on USB memory sticks, in case they are lost or stolen
- What steps you can take to hide information from physical or remote intruders

Pablo: *But my computer is already protected by the Windows login password! Isn't that good enough?*

Claudia: *Actually, Windows login passwords are usually quite easy to break. Plus, anybody who gets his hands on your computer for long enough to restart it with a LiveCD in the drive can copy your data without even having to worry about the password. If they manage to take it away for a while, then you're in even worse trouble. It's not just Windows passwords you need to worry about, either. You shouldn't trust Microsoft Word or Adobe Acrobat passwords either.*

Encrypting your information is a bit like keeping it in a locked safe. Only those who have a key or know the lock's combination (an encryption key or password, in this case) can access it. The analogy is particularly appropriate for **TrueCrypt** and tools like it, which create secure containers called 'encrypted volumes' rather than simply protecting one file at a time. You can put a large number of files into an encrypted volume, but these tools will not protect anything that is stored elsewhere on your computer or USB memory stick.

Hands-on: Get started with the *TrueCrypt Guide*

While other software can provide encryption that is equally strong, TrueCrypt was designed specifically to make this kind of secure file storage as simple as possible. Furthermore, its support for carrying encrypted volumes on portable storage devices, the fact that it is a **FOSS** tool, and the 'deniability' features described in the *Hiding your sensitive information* section below, give TrueCrypt a distinct advantage over many built-in proprietary encryption tools, such as Windows XP's 'bitlocker'.

Pablo: *Alright, now you have me worried. What about other users on the same computer? Does this mean they can read files in the 'My Documents' folder?*

Claudia: *I like the way you're thinking! If your Windows password doesn't protect you from intruders, how can it protect you from other people with accounts on the same computer? In fact, your My Documents folder is normally visible to anybody, so other users wouldn't even have to do anything clever to read your unencrypted files. You're right, though, even if the folder is made 'private,' you're still not safe unless you use some kind of encryption.*

Tips on using file encryption safely

Storing confidential data can be a risk for you and for the people you work with. Encryption reduces this risk but does not eliminate it. The first step to protecting sensitive information is to reduce how much of it you keep around. Unless you have a good reason to store a particular file, or a particular category of information within a file, you should simply delete it (see Chapter 6: How to destroy sensitive information for more information about how to do this securely). The second step is to use a good file encryption tool, such as TrueCrypt.

Claudia: *Well, maybe we don't actually need to store information that could identify the people who gave us these testimonies. What do you think?*

Pablo: *Agreed. We should probably write down as little of that as possible. Plus, we should think up a simple code we can use to protect names and locations that we absolutely have to record.*

Returning to the analogy of a locked safe, there are a few things you should bear in mind when using TrueCrypt and tools like it. No matter how sturdy your safe is, it won't do you a whole lot of good if you leave the door open. When your TrueCrypt volume is 'mounted' (whenever you can access the contents yourself), your data may be vulnerable, so you should keep it closed except when you are actually reading or modifying the files inside it.

There are a few situations when it is especially important that you remember not to leave your encrypted volumes mounted:

- Disconnect them when you walk away from your computer for any length of time. Even if you typically leave your computer running overnight, you need to ensure that you do not leave your sensitive files accessible to physical or remote intruders while you are gone.
- Disconnect them before putting your computer to sleep. This applies to both 'suspend' and 'hibernation' features, which are typically used with laptops but may be present on desktop computers as well.
- Disconnect them before allowing someone else to handle your computer. When taking a laptop through a security checkpoint or border crossing, it is important that you disconnect all encrypted volumes

and shut your computer down completely.

- Disconnect them before inserting an untrusted USB memory stick or other external storage device, including those belonging to friends and colleagues.
- If you keep an encrypted volume on a USB memory stick, remember that just removing the device may not immediately disconnect the volume. Even if you need to secure your files in a hurry, you have to dismount the volume properly, then disconnect the external drive or memory stick, then remove the device. You might want to practice until you find the quickest way to do all of these things.

If you decide to keep your TrueCrypt volume on a USB memory stick, you can also keep a copy of the TrueCrypt program with it. This will allow you to access your data on other people's computers. The usual rules still apply, however: if you don't trust the machine to be free of malware, you probably shouldn't be typing in your passwords or accessing your sensitive data.

HIDING YOUR SENSITIVE INFORMATION

One issue with keeping a safe in your home or office, to say nothing of carrying one in your pocket, is that it tends to be quite obvious. Many people have reasonable concerns about incriminating themselves by using encryption. Just because the legitimate reasons to encrypt data outnumber the illegitimate ones does not make this threat any less real. Essentially, there are two reasons why you might shy away from using a tool like TrueCrypt: the risk of self-incrimination and the risk of clearly identifying the location of your most sensitive information.

Considering the risk of self-incrimination

Encryption is illegal in some countries, which means that downloading, installing or using software of this sort might be a crime in its own right. And, if the police, military or intelligence services are among those groups from whom you are seeking to protect your information, then violating these laws can provide a pretext under which your activities might be investigated or your organisation might be persecuted. In fact, however, threats like this may have nothing to do with the legality of the tools in question. Any time that merely being associated with encryption software would be enough to expose you to accusations of criminal activity or espionage (regardless of what is actually inside your encrypted volumes), then you will have to think carefully about whether or not such tools are appropriate for your situation.

If that is the case, you have a few options:

- You can avoid using data security software entirely, which would require that you store only non-confidential information or invent a system of code words to protect key elements of your sensitive files.
- You can rely on a technique called steganography to hide your sensitive information, rather than encrypting it. There are tools that can help with this, but using them properly requires very careful preparation, and you still risk incriminating yourself in the eyes of anyone who learns what tool you have used.
- You can try to store all of your sensitive information in a secure webmail account, but this demands a reliable network connection and a relatively sophisticated understanding of computers and Internet services. This technique also assumes that network encryption is less incriminating than file encryption and that you can avoid accidentally copying sensitive data onto your hard drive and leaving it there.
- You can keep sensitive information off of your computer by storing it on a USB memory stick or portable hard drive. However, such devices are typically even more vulnerable than computers to loss and confiscation, so carrying around sensitive, unencrypted information on them is usually a very bad idea.

If necessary, you can employ a range of such tactics. However, even in circumstances where you are concerned about self-incrimination, it may be safest to use TrueCrypt anyway, while attempting to disguise your encrypted volume as best you can.

If want to make your encrypted volume less conspicuous, you can rename it to look like a different type of file. Using the '.iso' file extension, to disguise it as a CD image, is one option that works well for large volumes of around 700 MB. Other extensions would be more realistic for smaller volumes. This is a bit like hiding your safe behind a painting on the wall of your office. It might not hold up under close inspection, but it will offer some protection. You can also rename the **TrueCrypt** program itself, assuming you have stored it as you would a regular file on your hard drive or USB memory stick, rather than installing it as a program. The *TrueCrypt Guide* explains how to do this.

Considering the risk of identifying your sensitive information

Often, you may be less concerned about the consequences of 'getting caught' with **encryption** software on your computer or USB memory stick and more concerned that your encrypted volume will indicate precisely where you store the information that you most wish to protect. While it may be true that no one else can read it, an intruder will know that it is there, and that you have taken steps to protect it. This exposes

you to various non-technical methods through which that intruder might attempt to gain access, such as intimidation, blackmail, interrogation and torture. It is in this context that TrueCrypt's deniability feature, which is discussed in more detail below, comes into play.

TrueCrypt's deniability feature is one of the ways in which it goes beyond what is typically offered by file **encryption** tools. This feature can be thought of as a peculiar form of **steganography** that disguises your most sensitive information as other, less sensitive, hidden data. It is analogous to installing a subtle 'false bottom' inside that not-so-subtle office safe. If an intruder steals your key, or intimidates you into giving her the safe's combination, she will find some convincing 'decoy' material, but not the information that you truly care about protecting.

Only you know that your safe contains a hidden compartment in the back. This allows you to 'deny' that you are keeping any secrets beyond what you have already given to the intruder, and might help protect you in situations where you must reveal a password for some reason. Such reasons might include legal or physical threats to your own safety, or that of your colleagues, associates, friends and family members. The purpose of deniability is to give you a chance of escaping from a potentially dangerous situation even if you choose to continue protecting your data. As discussed in the *Considering the risk of self-incrimination* section, however, this feature is much less useful if merely being caught with a safe in your office is enough to bring about unacceptable consequences.

TrueCrypt's deniability feature works by storing a 'hidden volume' inside your regular encrypted volume. You open this hidden volume by providing an alternate password that is different from the one you would normally use. Even if a technically sophisticated intruder gains access to the standard volume, he will be unable to prove that a hidden one exists.

Of course, he may very well know that TrueCrypt is capable of hiding information in this way, so there is no guarantee that the threat will disappear as soon as you reveal your decoy password. Plenty of people use TrueCrypt without enabling its deniability feature, however, and it is generally considered impossible to determine, through analysis, whether or not a given encrypted volume contains this kind of 'false bottom'. That said, it is your job to make sure that you do not reveal your hidden volume through less technical means, such as leaving it open or allowing other applications to create shortcuts to the files that it contains. The *Further reading* section, below, can point you to more information about this.

Claudia: ***Alright, so let's toss some junk into the standard volume, and then we can move all our testimonies into the hidden one. Do you have some old PDFs or something we can use?***

Pablo: ***Well, I was thinking about that. I mean, the idea is for us to give up the decoy password if we have no other choice, right? But, for that to be convincing, we need to make sure those files look kind of important, don't you think? Otherwise, why would we bother to encrypt them? Maybe we should use some unrelated financial documents or a list of website passwords or something.***

FURTHER READING

- For additional information on securing your files, see the *Cryptology* chapter, the *Steganography* chapter and *Case Study 3* from the *Digital Security and Privacy for Human Rights Defenders* book [1].
- The *TrueCrypt FAQ* [2] provides answers to some common questions about TrueCrypt.

LINKS

[1] ***www.frontlinedefenders.org/manual/en/esecman***
[2] ***www.truecrypt.org/faq.php***

5
Recover from information loss

5. How to recover from information loss

Each new method of storing or transferring digital information tends to introduce several new ways in which the information in question can be lost, taken or destroyed. Years of work can disappear in an instant, as a result of theft, momentary carelessness, the confiscation of computer hardware, or simply because digital storage technology is inherently fragile. There is a common saying among computer support professionals: "it's not a question of if you will lose your data; it's a question of when." So, when this happens to you, it is extremely important that you already have an up-to-date backup and a well-tested means of restoring it. The day you are reminded about the importance of a backup system is generally the day after you needed to have one in place.

Although it is one of the most basic elements of secure computing, formulating an effective backup policy is not as simple as it sounds. It can be a significant planning hurdle for a number of reasons: the need to store original data and backups in different physical locations, the importance of keeping backups confidential, and the challenge of coordinating among different people who share information with one another using their own portable storage devices. In addition to backup and file-recovery tactics, this chapter addresses two specific tools, **Cobian Backup** and **Undelete Plus**.

Background scenario

Elena is an environmentalist in a Russian-speaking country, where she has begun to create a website that will rely on creative presentation of images, videos, maps and stories to highlight the extent of illegal deforestation in the region. She has been collecting documents, media files and geographic information about logging for years, and most of it is stored on an old Windows computer in the office of the NGO where she works. While designing a website around this information, she has come to realise its importance and to worry about preserving it in the event that her computer should be damaged, especially if it should happen before she gets everything copied up to the website. Other members of her organisation sometimes use the computer, so she also wants to learn how to restore her files if someone accidentally deletes the folder containing her work. She asks her nephew Nikolai to help her develop a backup strategy.

What you can learn from this chapter

- How to organise and back up your information
- Where you should store your backups
- How you can manage your backups securely
- How to recover files that have been deleted accidentally

IDENTIFYING AND ORGANISING YOUR INFORMATION

While it is clearly important that you take steps to prevent disaster, by making sure that your information is physically safe, free of malware and protected by a good **firewall** and strong passwords, on their own these steps are not enough. There are simply too many things that can go wrong, including virus attacks, **hackers**, electrical short circuits, power spikes, water spills, theft, confiscation, demagnetisation, operating system crashes and hardware failure, to name just a few. Preparing for disaster is just as important as defending against it.

Elena: *I know backup is important, Nikolai, but doesn't that mean I should have someone else set it up for me? I mean, am I really going to have the time, resources and expertise to do this on my own?*

Nikolai: *You'll be fine. Coming up with a good backup plan takes a bit of thought, but it doesn't take all that much time or money. And, compared with losing all of your information, you can hardly call it inconvenient, right? Besides, backup is definitely one of those things that you should manage yourself. Unless the people who normally help you out with tech support are extremely reliable and extremely well-informed about where you keep your digital information, you're better off setting things up on your own.*

The first step to formulating a ***backup policy*** is to picture where your personal and work information is currently located. Your email, for example, may be stored on the provider's mail server, on your own computer, or in both places at once. And, of course, you might have several email accounts. Then, there are important documents on the computers you use, which may be in the office or at home. There are address books, chat histories and personal program settings. It is also possible that some information is stored on removable media as well, including USB memory sticks, portable hard drives, CDs, DVDs, and old floppy disks. Your mobile phone contains a list of contacts and may have important text messages stored in it. If you have a website, it may contain a large collection of articles built up over years of work. And, finally, don't forget your non-digital information, such as paper notebooks, diaries and letters.

Next, you need to define which of these files are 'master copies,' and which are duplicates. The master copy is generally the most up-to-date version of a particular file or collection of files, and corresponds to copy that you would actually edit if you needed to update the content. Obviously, this distinction does not apply to files of which you have only one copy, but it is extremely important for certain types of information. One common disaster scenario occurs when only duplicates of an important document are backed up, and the master copy itself gets lost or destroyed before those duplicates can be updated. Imagine, for example, that you have been travelling for a week while updating the copy of a particular spreadsheet that you keep on your USB memory stick. At this point, you should begin thinking of that copy as your master copy, because the periodic, automated backups of the outdated version on your office computer are no longer useful.

Try to write down the physical location of all master and duplicate copies of the information identified above. This will help you clarify your needs and begin to define an appropriate backup policy. The table below is a very basic example. Of course, you will probably find that your list is much longer, and contains some 'storage devices' with more than one 'data type' and some data types that are present on multiple devices.

Data Type	Master/ Duplicate	Storage Device	Location
Electronic documents	Master	Computer hard drive	Office
A few important electronic documents	Duplicate	USB memory stick	With me
Program databases (photos, address book, calendar, etc.)	Master	Computer hard drive	Office
A few electronic documents	Duplicate	CDs	Home
Email & email contacts	Master	Gmail account	Internet
Text messages & phone contacts	Master	Mobile phone	With me
Printed documents (contracts, invoices, etc.)	Master	Desk drawer	Office

In the table above, you can see that:

- The only documents that will survive if your office computer's hard drive crashes are the duplicates on your USB memory stick and the CD copies at home.
- You have no offline copy of your email messages or your address book, so if you forget your password (or if someone manages to

change it maliciously), you will lose access to them.
- You have no copies of any data from your mobile phone.
- You have no duplicate copies, digital or physical, of printed documents such as contracts and invoices.

DEFINING YOUR BACKUP STRATEGY

To back up all of the data types listed above, you will need a combination of software and process solutions. Essentially, you need to make sure that each data type is stored in at least two separate locations.

Electronic documents

Create a full backup of the documents on your computer using a program like **Cobian Backup**, which is described in more detail below. Store the backup on something portable so that you can take it home or to some other safe location. It may be easier to use CDs or DVDs for this, rather than a portable hard drive or USB memory stick, so that you do not risk losing your old backups while you are transporting a new one. Blank CDs may be cheap enough that you can use a new one every time you make a backup. Because this category of data often contains the most sensitive information, it is particularly important that you protect your electronic document backups using encryption. You can learn how to do this in *Chapter 4: How to protect the sensitive files on your computer* and in the *TrueCrypt Guide*.

Program databases

Once you have determined the location of your program databases, you can back them up in the same way as electronic documents.

Email

Rather than accessing your email only through a web browser, install an email client like **Thunderbird** and configure it to work with your account. Most webmail services will provide instructions on how to use such programs and, often, how to import your email addresses into them. You can learn more about this in the Further Reading section, below. Make sure that you leave a copy of your messages on the mail server, rather than just moving them over to your computer. The *Thunderbird Guide* explains in detail how to do this.

Mobile phone contents

To back up the phone numbers and text messages on your mobile phone, you can connect it to your computer using the appropriate software, which is generally available from the website of the company that manufactured your phone. You may need to buy a special USB cable to do this, however. As an alternative, you can use the phone to copy your text messages and contact information from your **SIM card** onto the phone itself, and then copy them onto a backup SIM card. This method can be particularly useful as an emergency backup solution, but remember to keep the extra SIM card safe. The ability to copy contact information and text messages between a mobile phone and its SIM card is a standard feature, but if your phone allows you to store this kind of information on a removable flash memory card instead, then backing it up may be even easier.

Printed documents

Where possible, you should scan all of your important papers, then back them up along with your other electronic documents, as discussed above.

In the end, you should have rearranged your storage devices, data types and backups in a way that makes your information much more resistant to disaster:

Data Type	Master/Duplicate	Storage Device	Location
Electronic documents	Master	Computer hard drive	Office
Electronic documents	Duplicate	CDs	Home
A few important electronic documents	Duplicate	USB memory stick	With me

Data Type	Master/ Duplicate	Storage Device	Location
Program databases	Master	Computer hard drive	Office
Program databases	Duplicate	CDs	Home

Data Type	Master/ Duplicate	Storage Device	Location
Email & email contacts	Duplicate	Gmail account	Internet
Email & email contacts	Master	Thunderbird on office computer	Office

Data Type	Master/ Duplicate	Storage Device	Location
Text messages & mobile phone contacts	Master	Mobile phone	With me
Text messages & mobile phone contacts	Duplicate	Computer hard drive	Office
Text messages & mobile phone contacts	Duplicate	Backup SIM	Home

Data Type	Master/Duplicate	Storage Device	Location
Printed documents	Master	Desk drawer	Office
Scanned documents	Duplicate	CDs	At home

Elena: *I know some people who keep all of their important documents on Gmail, by attaching them to 'draft' messages or emails to themselves. Would that count as a 'second physical location' for my files?*

Nikolai: *It might help you recover if you lose one or two very important documents, but it's pretty awkward. Honestly, how many documents per week would you be willing to back up like that? Plus, you need to consider whether or not those attachments are safe, especially if you're at all worried about your email being monitored. Unless you're connecting to Gmail securely, this is a bit like handing over your sensitive information on a silver platter. Using an HTTPS connection to Gmail in order to back up small Truecrypt volumes or KeePass database files would be pretty safe, because they're encrypted, but I really wouldn't recommend this as a general-purpose backup strategy.*

CREATING A DIGITAL BACKUP

Of the various data types discussed here, it is the 'electronic documents' that people tend to worry about most when establishing a backup policy. This term is somewhat ambiguous, but generally refers to files that you keep track of yourself and that you open manually, either by double-clicking on them or by using a particular application's File menu. Specifically, it includes text files, word processing documents, presentations, PDFs and spreadsheets, among other examples. Unlike email messages, for example, electronic documents are generally not synchronised with remote copies over the Internet.

When backing up your electronic documents, you should remember to back up your program databases, as well. If you use a calendar application or an electronic address book, for example, you will need to find the folder in which these programs store their data. Hopefully, these databases will be in the same location as your electronic documents, as they are often kept inside your My Documents folder on a Windows computer. If that is not the case, however, you should add the appropriate folders to your regular backup.

Email stored by an application such as **Thunderbird** is a special example of a program database. If you use an email program, especially if you are unable or unwilling to store a copy of your messages on the server, then you must ensure that this email database is included in your regular backup. You may consider image and video files to be electronic documents or items within a program database, depending on how you interact with them.

Applications like Windows Media player and iTunes, for example, work like databases. If you use programs like this, you might have to search your hard drive to learn where they store the actual media files that they help manage.

Storage devices

Before you can back up your electronic documents, you must decide what kind of storage device you will use.

Compact Discs (CDs)

CDs store around 700 Megabytes (MB) of data. You will need a CD burner and blank discs in order to create a CD backup. If you want to erase a CD and update the files stored on it, you will need to have a CD-RW burner and rewritable CDs. All major operating systems, including Windows XP, now include built-in software that can write CDs and CD-RWs. Keep in mind that the information written on these discs may begin to deteriorate after five or ten years. If you need to store a backup for longer than that, you will have to recreate the CDs occasionally, buy special 'long life' discs or use a different backup method.

Digital Video Discs (DVDs)

DVDs store up to 4.7 Gigabytes (GB) of data. They work much like CDs but require slightly more expensive equipment. You will need a DVD or DVD-RW burner, and appropriate discs. As with a CD, the data written on a normal DVD will eventually begin to fade.

USB memory sticks

A USB memory stick holds as much information as the capacity of the device allows. USB memory sticks can be quite inexpensive, even those with a capacity equal to or greater than that of a CD or DVD, and they are easy to erase or overwrite numerous times. Like CDs and DVDs, USB memory sticks have a limited lifetime, which is generally estimated to be around 10 years.

Remote server

A well-maintained network backup server may have almost unlimited capacity, but the speed and stability of your own Internet connection will determine whether or not this is a realistic option. Keep in mind that running a backup server in your own office, while faster than copying information over the Internet, violates the requirement that you keep a copy of your important data in two different physical locations. There are free storage services on the Internet, as well, but you should always encrypt your backups before uploading them to servers run by organisations or individuals whom you do not know and trust. See the *Further reading* section for a few examples.

Backup Software

Cobian Backup is a user-friendly tool that can be set to run automatically, at regularly scheduled times, and to include only files that have changed since your last backup. It can also compress backups to make them smaller.

Hands-on: Get started with the *Cobian Backup Guide*

As always, it is a good idea to encrypt your backup files using a tool such as TrueCrypt. More information about about data encryption can be found in *Chapter 4: How to protect the sensitive files on your computer*.

Hands-on: Get started with the *TrueCrypt Guide*

When using these backup tools, there are a few things you can do to help your backup system work smoothly:

- Organise the files on your computer. Try to move all of the folders that contain electronic documents you intend to back up into a single location, such as inside the My Documents folder.
- If you use software that stores its data in an application database, you should first determine the location of that database. If it is not in a convenient location, see if the program will allow you to choose a new location for its database. If it does, you can put it in the same folder as your electronic documents.
- Create a regular schedule to perform your backup.
- Try to establish procedures for all of the staff in your office who do not already have a reliable, secure backup policy. Help your coworkers understand the importance of this issue.
- Make sure to test the process of recovering data from your backup. Remember that, in the end, it is the restore procedure, not the backup procedure, that you really care about!

Elena: ***Alright, so I made an encrypted backup while I was at work, and I put it on a CD. Cobian is scheduled to update my backup in a few days. My desk at work has a drawer that locks, and I'm planning to keep these backup CDs in there so they won't get lost or broken.***
Nikolai: ***But what if your office burns down? Computer, desk, backup CDs and all? Or, what if your website forum gets used to plan some giant environmental demonstration, the authorities crack down, things get out of hand, and the organisation is raided? I doubt your little desk lock will keep the police from confiscating those CDs. What about keeping them at home, or asking a friend to store them for you?***

RECOVERING FROM ACCIDENTAL FILE DELETION

When you delete a file in Windows, it disappears from view, but its contents remain on the computer. Even after you empty the **Recycle Bin**, information from the files you deleted can usually still be found on the hard drive. See *Chapter 6: How to destroy sensitive information* to learn more about this.

Occasionally, if you accidentally delete an important file or folder, this security vulnerability can work to your advantage. There are several programs that can restore access to recently-deleted files, including a **FOSS** tool called **Undelete Plus**.

Hands-on: Get started with the *Undelete Plus Guide*

These tools do not always work, because Windows may have written new data over your deleted information. Therefore, it is important that you do as little as possible with your computer between deleting a file and attempting to restore it with a tool like Undelete Plus. The longer you use your computer before attempting to restore the file, the less likely it is that you will succeed. This also means that you should install data recovery software well ahead of time. If you have to install it after you've deleted an important file, there is some chance that the software itself will overwrite the critical data that you are trying to recover.

While it might sound like a lot of work to implement the policies and learn the tools described in this chapter, maintaining your backup strategy, once you have a system in place, is much easier than setting it up for the first time. And, given that backup may be the single most important aspect of data security, you can rest assured that going through this process is well worth the effort.

FURTHER READING

- More information on backup and data recovery can be found in the *Information Backup, Destruction and Recovery* chapter of the *Digital Security and Privacy for Human Rights Defenders* [1] book.
- There are several free online data storage services that provide a convenient way to back up a small amount of sensitive information,

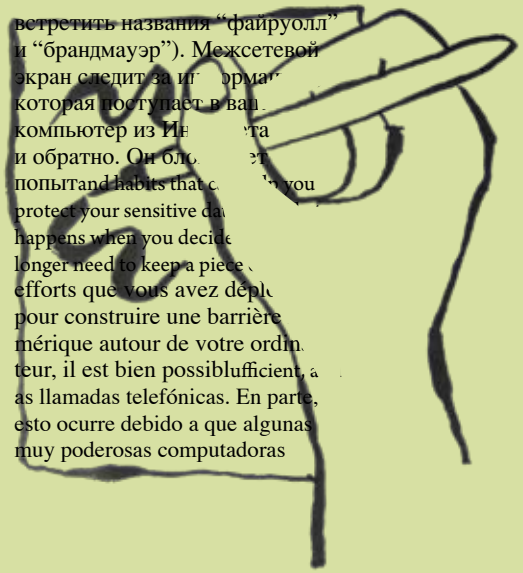
as long as you encrypt it first. *Dropbox* [2] and *ADrive* [3] are good examples of such a service.

- There is an excellent article on data recovery in *Wikipedia* [4].

LINKS

[1] ***www.frontlinedefenders.org/manual/en/esecman***
[2] ***https://www.getdropbox.com***
[3] ***www.adrive.com***
[4] ***www.en.wikipedia.org/wiki/Data_recovery***

6
Destroy sensitive information



встретить названия “файруолл” и “брандмауэр”). Межсетевой экран следит за ин ормаи которая поступает в ваш компьютер из Ин та и обратно. Он бло ет попытand habits that c you protect your sensitive da happens when you decid longer need to keep a piece efforts que vous avez dépl pour construire une barrière mérique autour de votre ordin teur, il est bien possiblufficient, a as llamadas telefónicas. En parte, esto ocurre debido a que algunas muy poderosas computadoras

6. How to destroy sensitive information

The previous chapters have discussed a number of tools and habits that can help you protect your sensitive data, but what happens when you decide that you no longer need to keep a piece of information? If you determine, for example, that your encrypted backup copies of a particular file are sufficient, and you want to delete the master, what is the best way to do so? Unfortunately, the answer is more complicated than you might think. When you delete a file, even after you empty the Recycle bin, the contents of that file remain on your hard drive and can be recovered by anyone who has the right tools and a little luck.

In order to ensure that deleted information does not end up in the wrong hands, you will have to rely on special software that removes data securely and permanently. **Eraser** is one such tool, and is discussed below. Using Eraser is a bit like shredding a paper document rather than simply tossing it into a bin and hoping that nobody finds it. And, of course, deleting files is only one example of a situation in which you might need to destroy sensitive data. If you consider the details that someone, particularly a powerful, politically-motivated adversary, could learn about you or your organisation by reading certain files that you thought you had deleted, you will probably think of a few more examples of data that you'd like to permanently erase, by destroying outdated backups, wiping old hard drives before giving them away, deleting old user accounts, and clearing your web browsing history, for example.

CCleaner, the other tool described in this chapter, can help you face the challenge of deleting the many temporary files that your operating system and applications create every time you use them.

Background scenario

Elena is an environmentalist in a Russian-speaking country, where she maintains an increasingly-popular website that highlights the extent of illegal deforestation in the region. She has created a backup of the information used to create the website, and she keeps copies of it at home, in the office and on her new laptop. Recently, she has also begun to store a copy of the webserver's visitor logs and the database containing her users' forum posts. Elena will soon be travelling internationally, to attend a large global conference of environmental activists, some of whom have reported having their laptops taken away for over an hour at border-crossings. To protect her

sensitive information, and the safety of her more political forum participants, she has moved her home and office backups onto a TrueCrypt volume and removed the copy from her laptop. She asked her nephew Nikolai for advice, and he has warned her that she needs to do more than just delete her old backup if she is worried about having her computer seized by border officials.

What you can learn from this chapter

- How to remove sensitive information from your computer permanently
- How to remove information stored on removable storage devices like CDs and USB memory sticks
- How to prevent someone from learning what documents you have previously been viewing on your computer
- How to maintain your computer so that deleted files cannot be recovered in the future

DELETING INFORMATION

From a purely technical perspective, there is no such thing as a delete function on your computer. Of course, you can drag a file to the Recycle Bin and empty the bin, but all this really does is clear the icon, remove the file's name from a hidden index of everything on your computer, and tell Windows that it can use the space for something else. Until it actually does use that space, however, the space will be occupied by the contents of the deleted information, much like a filing cabinet that has had all of its labels removed but still contains the original files. This is why, if you have the right software and act quickly enough, you can restore information that you've deleted by accident, as discussed in *Chapter 5: How to recover from information loss*.

You should also keep in mind that files are created and insecurely deleted, without your knowledge, every time you use your computer. Suppose, for example, that you are writing a large report. It may take you a week, working several hours each day, and every time the document is saved, Windows will create a new copy of the document and store it on your hard drive. After a few days of editing, you may have unknowingly saved several versions of the document, all at different stages of completion.

Windows generally deletes the old versions of a file, of course, but it does not look for the exact location of the original in order to overwrite it securely when a new copy is made. Instead, it simply puts the latest version into a new section of the metaphorical filing cabinet mentioned above, moves the label from the old section to the new one, and leaves the previous draft where it was until some other program needs to use that space. Clearly, if you have a good reason to destroy all traces of that document from your filing cabinet, removing the latest copy is not going to be enough, and simply throwing away the label would be even worse.

Remember, too, that computer hard drives are not the only devices that store digital information. CDs, DVDs, USB memory sticks, floppy disks, flash memory cards from mobile phones and removable hard drives all have the same issues, and you should not trust a simple delete or rewrite operation to clear sensitive information from any of them.

WIPING INFORMATION WITH SECURE DELETION TOOLS

When you use a secure deletion tool, such as those recommended in this chapter, it would be more accurate to say that you are replacing, or 'overwriting,' your sensitive information, rather than simply deleting it. If you imagine that the documents stored in those hypothetical filing cabinet discussed above are written in pencil, then secure deletion software not only erases the content, but scribbles over the top of every word. And, much like pencil lead, digital information can still be read, albeit poorly, even after it has been erased and something has been written over the top of it. Because of this, the tools recommended here overwrite files with random data several times. This process is called **wiping**, and the more times information is overwritten, the more difficult it becomes for someone to recover the original content. Experts generally agree that three or more overwriting passes should be made; some standards recommend seven or more. Wiping software automatically makes a reasonable number of passes, but you can change that number if you like.

Wiping files

There are two common ways to **wipe** sensitive data from your hard drive or storage device. You can wipe a single file or you can wipe all of the 'unallocated' space on the drive. When making this decision, it may be helpful to think about the other hypothetical example proposed earlier--the long report that may have left incomplete copies scattered throughout your hard drive even though only one file is visible. If you wipe the file itself, you guarantee that the current version is completely removed, but you leave the other copies where they are. In fact, there is no way to target those copies directly, because they are not visible without special software. By wiping all of the blank space on your storage device, however, you ensure that all previously-deleted information is

destroyed. Returning to the metaphor of the poorly-labeled file cabinet, this procedure is comparable to searching through the cabinet, then erasing and scribbling repeated over any documents that have already had their labels removed.

Eraser is a free and open-source secure deletion tool that is extremely easy to use. You can wipe files with Eraser in three different ways: by selecting a single file, by selcting the contents of the Recycle Bin, or by wiping all unallocated space on the drive. Eraser can also wipe the contents of the Windows swap file, which is discussed below.

Hands-on: Get started with the *Eraser Guide*

While secure deletion tools will not damage any visible files unless you explicitly wipe them, it is still important to be careful with software like this. After all, accidents happen, which is why people find **Recycle Bins** and data recovery tools so useful. If you get accustomed to wiping your data every time you delete something, you may find yourself with no way to recover from a simple mistake. Always make sure you have a secure backup before wiping large amounts of data from your computer.

Elena: *I know word processing programs like Microsoft Word and Open Office sometimes make temporary copies of a file while you're working on it. Do other programs do that too, or should I mostly just worry about files that I create and delete myself?*

Nikolai: *Actually, there are lots of places on your computer where programs leave traces of your personal information and online activities. I'm talking about websites you've visited, draft emails you've worked on recently and other things like that. All of this stuff could be sensitive, depending on how often you use that computer.*

Wiping temporary data

The feature that allows **Eraser** to **wipe** all unallocated space on a drive is not as risky as it might sound, because it only wipes previously-deleted content. Normal, visible files will be unaffected. On the other hand, this very fact serves to highlight a separate issue: Eraser can not help you clean up sensitive information that has not been deleted, but that may be extremely well-hidden. Files containing such data may be tucked away in obscure folders, for example, or stored with meaningless filenames. This is not a major issue for electronic documents, but can be very important for information that is collected automatically whenever you use your computer. Examples include:

- Temporary data recorded by your browser while displaying webpages, including text, images, **cookies**, account information, personal data used to complete online forms and the history of which websites you have visited.
- Temporary files saved by various applications in order to help you recover should your computer crash before you can save your work. These files might contain text, images, spreadsheet data and the names of other files, along with other potentially sensitive information.
- Files and links stored by Windows for the sake of convenience, such as shortcuts to applications you have used recently, obvious links to folders that you might prefer to keep hidden and, of course, the contents of your **Recycle Bin** should you forget to empty it.
- The Windows **swap file**. When your computer's memory is full, for example when you have been running several programs at the same time on an older computer, Windows will sometimes copy the data you are using into a single large file called the swap file. As a result, this file might contain almost anything, including webpages, document content, passwords or encryption keys. Even when you shut down your computer, the swap file is not removed, so you must wipe it manually.

In order to remove common temporary files from your computer, you can use a freeware tool called **CCleaner**, which was designed to clean up after software like Internet Explorer, Mozilla Firefox and Microsoft Office applications (all of which are known to expose potentially sensitive information), as well as cleaning Windows itself. CCleaner has the ability to delete files securely, which saves you from having to wipe unallocated drive space, using **Eraser**, after each time you run it.

Hands-on: Get started with the *CCleaner Guide*

TIPS ON USING SECURE DELETION TOOLS EFFECTIVELY

You are now familiar with a few of the ways in which information might be exposed on your computer or storage device, even if you are dilligent about erasing sensitive files. You also know what tools you can use to wipe that information permanently. There are a few simple steps that you should follow, especially if it is your first time using these tools, in order to ensure that your drive is cleaned safely and effectively:

1. Create an encrypted backup of your important files, as discussed in *Chapter 5: How to recover from information loss.*

2. Close down all unnecessary programs and disconnect from the Internet.
3. Delete all unnecessary files, from all storage devices, and empty the **Recycle Bin**
4. **Wipe** temporary files using CCleaner.
5. Wipe the Windows swap file using Eraser.
6. Wipe all of the free space on your computer and other storage devices using Eraser. You might need to let this procedure run overnight, as it can be quite slow.

You should then get into the habit of:

- Periodically using **CCleaner** to **wipe** temporary files
- Wiping sensitive electronic documents using **Eraser**, instead of using the Recycle Bin or the Windows delete function
- Periodically using Eraser to wipe the Windows **swap file**
- Periodically using Eraser to wipe all unallocated space on your hard drives, USB memory sticks, and any other storage devices that may have had sensitive information deleted from them recently. This might include floppy disks, rewritable CDs, rewritable DVDs and removable flash memory cards from cameras, mobile phones or portable music players.

TIPS ON WIPING THE ENTIRE CONTENTS OF A STORAGE DEVICE

You might occasionally need to **wipe** a storage device completely. When you sell or give away an old computer, it is best to remove the hard drive and let the computer's new owner acquire one for herself. If this is not an option, however, you should at least wipe the drive thoroughly with **Eraser** before handing it over. And, even if you do keep the drive, you will probably want to wipe it anyway, regardless of whether you intend to reuse or discard it. Similarly, if you purchase a new hard drive, you should wipe your old one after copying your data and making a secure backup. If you are intending to throw away or recycle an old drive, you should also consider destroying it physically. (Many computer support professionals recommend a few strong blows with a hammer before discarding any data-storage device that once contained sensitive information.)

In any of the situations described above, you will need to use Eraser to wipe an entire hard drive, which is impossible as long as the operating system is running on that particular drive. The easiest way to get around this issue is to remove the drive and put it into an external USB 'drive enclosure,' which you can then plug into any computer with Eraser installed on it. At that point, you can delete the full contents of the external drive and then use Eraser to wipe all of its unallocated space. Fortunately, this is not something you will have to do often, as it may take quite some time.

Rather than trying to wipe data that have been stored on a rewritable CD or DVD, it is often better to destroy the disc itself. If necessary, you can create a new one containing any information you wish to keep. And, of course, this is the only way to 'erase' content from a non-rewritable disc. It is surprisingly difficult to destroy the contents of a CD or DVD completely. You may have heard stories about information being recovered from such discs even after they were cut into small pieces. While these stories are true, reconstructing information in this way takes a great deal of time and expertise. You will have to judge for yourself whether or not someone is likely to expend that level of resources in order to access your data. Typically, a sturdy pair of scissors (or a very sturdy paper shredder) will do the job nicely. If you want to take extra precautions, you can mix up the resulting pieces and dispose of them in various locations far from your home or office.

Elena: ***I still have an old CD backup of the webserver logs, and I heard that you can erase a CD by putting it in the microwave. Somehow, though, it sounds like a really bad idea to me. Do people really do that? Does it work?***

Nikolai: ***I imagine it destroys the data pretty effectively, but I wouldn't know, because I'd never put a CD in my microwave! You're right. That sounds like a terrible idea. Even if the metal doesn't damage your microwave or start a fire, I bet that plastic would give off some pretty unhealthy fumes. Come to think of it, I wouldn't recommend burning CDs in a fire, either.***

FURTHER READING

- While it does not use secure deletion techniques to wipe them permanently, Firefox does provide a built-in way to clear many of its own temporary files. This feature is described in the *Firefox Guide* and on the *Firefox website* [1].
- The *CCleaner FAQ* [2] provides additional information about installing and using the tool.
- Although much of the paper is quite technical, the introduction of Peter Guttmann's *Secure Deletion of Data from Magnetic and Solid-State Memory* [3] is worth reading, as the *method* [4] he describes has had a major influence on the developers of Eraser and other secure file removal tools.

LINKS

[1] *https://support.mozilla.com/en-US/kb/Clearing+Private+Data*
[2] *www.ccleaner.com/help/faq*
[3] *www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/*
[4] *www.en.wikipedia.org/wiki/Gutmann_method*

7
Keep your Internet communication private

7. How to keep your Internet communication private

The convenience, cost-effectiveness and flexibility of email and instant messaging make them extremely valuable for individuals and organizations with even the most limited access to the Internet. For those with faster and more reliable connections, software such as **Skype** and other ***Voice-over-IP*** (**VoIP**) tools also share these characteristics. Unfortunately, these digital alternatives to traditional means of communication can not always be relied upon to keep sensitive information private. Of course, this is nothing new. Postal mail, telephone calls and text messages are all vulnerable as well, particularly when used by those who may have been targeted for surveillance by the authorities.

One important difference between digital, Internet-based communication techniques and more traditional methods, is that the former often allow you to determine your own level of security.

If you send emails, instant messages and VoIP conversations using insecure methods, they are almost certainly less private than letters or telephone calls. In part, this is because a few powerful computers can automatically search through a large amount of digital information to identify senders, recipients and specific key words. Greater resources are required to carry out the same level of surveillance on traditional communication channels. However, if you take certain precautions, the opposite can be true. The flexibility of Internet communication tools and the strength of modern **encryption** can now provide a level of privacy that was once available only to national military and intelligence organizations.

By following the guidelines and exploring the software discussed in this chapter, you can greatly improve your communication security. The **Riseup** email service, the Off the Record (**OTR**) plugin for the **Pidgin** instant messaging program, Mozilla **Firefox** and the **Enigmail** add-on for the Mozilla **Thunderbird** email client are all excellent tools. While using them, however, you should keep in mind that the privacy of a given conversation is never one hundred percent guaranteed. There is always some threat that you did not consider, be it a **keylogger** on your computer, a person listening at the door, a careless email correspondent or something else entirely.

The goal of this chapter is to help you reduce even the threats that do not occur to you, while avoiding the extreme position, favoured by some, that you should not send anything over the Internet that you are not willing to make public.

Background scenario

Claudia and Pablo work with a human rights NGO in a South American country. After spending several months collecting testimonies from witnesses to the human rights violations that have been committed by the military in their region, Claudia and Pablo have begun taking steps to protect the resulting data. They have kept only the information they need, which they store in a TrueCrypt partition that is backed up in several physical locations. While preparing to publish certain aspects of these testimonies in a report, they have found that they must discuss sensitive information with a few of their colleagues in another country. Although they have agreed not to mention names or locations, they still want to ensure that their email and instant messaging conversations on this topic remain private. After calling a meeting to discuss the importance of communication security, Claudia has asked if anyone in the office has questions.

What you can learn from this chapter

- Why most webmail and instant messaging services are not secure
- How to create a new and more secure email account
- How to improve the security in your current email account
- How to use a secure instant messaging service
- What to do if you think someone might be accessing your email
- How to verify the identity of an email correspondent

SECURING YOUR EMAIL

There are a few important steps that you can take in order to increase the security of your email communication. The first is to make sure that only the person to whom you send a given message is able to read it. This is discussed in the *Keeping your webmail private* and *Switching to a more secure email account* sections, below. Going beyond the basics, it is sometimes critical that your email contacts have the ability to verify, without a doubt, that a particular message truly came from you and not from someone who might be attempting to impersonate you. One way to accomplish this is described under *Advanced email security*, in the *Encrypting and authenticating individual email messages* section.

You should also know what to do if you think the privacy of your email account may have been violated. The *Tips on responding to suspected email surveillance* section addresses this question.

Remember, too, that secure email will not do you any good if everything you type is recorded by spyware and periodically sent over the Internet to a third party. *Chapter 1: How to protect your computer from malware and hackers* offers some advice on how to prevent this sort of thing, and *Chapter 3: How to create and maintain secure passwords* will help you protect your accounts for the email and instant messaging tools described below.

Keeping your webmail private

The Internet is an open network through which information typically travels in a readable format. If a normal email message is intercepted on the way to a recipient, its contents can be read quite easily. And, because the Internet is just one large, worldwide network that relies on intermediary computers to direct traffic, many different people may have the opportunity to intercept a message in this way. Your ***Internet Service Provider*** (**ISP**) is the first recipient of an email message as it begins its journey to the recipient. Similarly, the recipient's ISP is the last stop for your message before it is delivered. Unless you take certain precautions, your messages can be read or tampered with at either of these points, or anywhere in between.

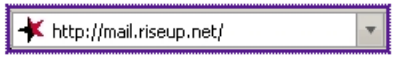
Pablo: ***I was talking to one of our partners about all this, and she said that she and her colleagues sometimes just save important messages in the 'Drafts' folder of a webmail account where they all share a password. It sounds kind of strange to me, but would it work? I mean, wouldn't that prevent anyone from reading the messages, since they're never actually sent?***

Claudia: ***Any time you read an email on your computer, even if it's just a 'draft', its contents have been sent to you over the Internet. Otherwise, it couldn't appear on your screen, right? The thing is, if someone has you under surveillance, they don't just monitor your email messages, they can scan all readable information going to and from your computer. In other words, this trick wouldn't work unless everyone connects securely to that shared webmail account. And, if they do, then it really doesn't hurt to create separate accounts or to go ahead and hit that 'send' button.***

It has long been possible to secure the Internet connection between your computer and the websites that you visit. You often encounter this level of security when entering passwords or credit card information into websites. The technology that makes it possible is called ***Secure Sockets Layer*** (**SSL**) **encryption**. You can tell whether or not you are

using SSL by looking closely at your Web browser's address bar.

All Web addresses normally begin with the letters **HTTP**, as can be seen in the example below:



When you are visiting a secure website, its address will begin with **HTTPS**.

The extra **S** on the end signifies that your computer has opened a secure connection to the website. You may also notice a 'lock' symbol, either in the **address bar** or in the **status bar** at the bottom of your browser window. These are clues to let you know that anyone who might be monitoring your Internet connection will no longer be able to eavesdrop on your communication with that particular website.

In addition to protecting passwords and financial transactions, this type of **encryption** is perfect for securing your webmail. However, many webmail providers do not offer secure access, and others require that you enable it explicitly, either by setting a preference or by typing in the **HTTPS** manually. You should always make sure that your connection is secure before logging in, reading your email, or sending a message.

You should also pay close attention if your browser suddenly begins to complain about invalid **security certificates** when attempting to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages. Finally, if you rely on webmail to exchange sensitive information, it is important that your browser be as reliable as possible. Consider installing Mozilla Firefox and its security-related add-ons.

Hands-on: Get started with the *Firefox Guide*

Pablo: ***One of the guys who's going to be working on this report with us tends to use his Yahoo webmail account when he's not in the office. And I seem to remember somebody else using Hotmail. If I send a message to these guys, can other people read it?***

Claudia: ***Probably. Yahoo, Hotmail and plenty of other webmail providers have insecure websites that don't protect the privacy of their users' messages. We're going to have to change some people's habits if we want to be able to discuss these testimonies securely.***

Switching to a more secure email account

Few webmail providers offer **SSL** access to your email. Yahoo and Hotmail, for instance, provide a secure connection while you log in, to protect your password, but your messages themselves are sent and received insecurely. In addition, Yahoo, Hotmail and some other free webmail providers insert the **IP address** of the computer you are using into all of the messages you send.

Gmail accounts, on the other hand, can be used entirely through a secure connection, as long as you login to your account from ***https://mail.google.com*** (with the **HTTPS**), rather than ***http://mail.google.com***. In fact, you can now set a preference that tells Gmail always to use a secure connection. And, unlike Yahoo or Hotmail, Gmail avoids revealing your **IP address** to email recipients. However, it is not recommend that you rely entirely on Google for the confidentiality of your sensitive email communication. Google scans and records the content of its users' messages for a wide variety of purposes and has, in the past, conceded to the demands of governments that restrict digital freedom. See the ***Further reading*** section for more information about Google's privacy policy.

If possible, you should create a new **Riseup** email account by visiting ***https://mail.riseup.net***. Riseup offers free email to activists around the world and takes great care to protect the information stored on their servers. They have long been a trusted resource for those in need of secure email solutions. And, unlike Google, they have very strict policies regarding their users' privacy and no commercial interests that might some day conflict with those policies. In order to create a new Riseup account, however, you will need two 'invite codes.' These codes can be given out by anyone who already has a Riseup account. If you have a bound copy of this booklet, you should have received your 'invite codes' along with it. Otherwise, you will need to find two Riseup users and ask them each to send you a code.

Hands-on: Get started with the *Riseup Guide*

Both Gmail and Riseup are more than just webmail providers. They can also be used with an email client, such as Mozilla **Thunderbird**, that supports the techniques described under *Advanced email security*. Ensur-

ing that your email client makes an **encrypted** connection to your provider is just as important as accessing your webmail through **HTTPS**. If you use an email client, see the Thunderbird Guide for additional details. A the very least, however, you should be sure to enable SSL or encryption for both your incoming and outgoing mail servers.

Pablo: *So, should I switch to using Riseup or I can keep using Gmail, and just switch to the secure 'https' address?*

Claudia: *It's your call, but there are a few things you should definitely consider when choosing an email provider. First, do they offer a secure connection to your account? Gmail does, so you're OK there. Second, do you trust the administrators to keep your email private and not to read through it or share it with others? That one's up to you. And, finally, you need to think about whether or not it's acceptable for you to be identified with that provider. In other words, will it get you in trouble to use an email address that ends in 'riseup.net', which is known to be popular among activists, or do you need a more typical 'gmail.com' address?*

Regardless of what secure email tools you decide to use, keep in mind that every message has a sender and one or more recipients. You yourself are only part of the picture. Even if you access your email account securely, consider what precautions your contacts may or may not take when sending, reading and replying to messages. Try to learn where your contacts' email providers are located, as well. Naturally, some countries are more aggressive than others when it comes to email surveillance. To ensure private communication, you and your contacts should all use secure email services hosted in relatively safe countries. And, if you want to be certain that messsages are not intercepted between your email server and a contact's email server, you might all choose to use accounts from the same provider. **Riseup** is one good choice.

Additional tips on improving your email security

- Always use caution when opening email attachments that you are not expecting, that come from someone you do not know or that contain suspicious subject lines. When opening emails like this, you should ensure that your anti-virus software is up-to-date and pay close attention to any warnings displayed by your browser or email program.
- Using anonymity software like **Tor**, which is described in *Chapter 8: How to remain anonymous and bypass censorship on the Internet*, can help you hide your chosen email service from anyone who might be monitoring your Internet connection. And, depending on the extent of Internet filtering in your country, you may need to use Tor, or one of the other circumvention tools described in chapter 8, just to access a secure email provider such as Riseup or Gmail.
- When creating an account that you intend to use while remaining anonymous from your own email recipients, or from public forums to which you might post messages by email, you must be careful not to register a username or 'Full Name' that is related to your personal or professional life. In such cases, it is also important that you avoid using Hotmail, Yahoo, or any other webmail provider that includes your **IP address** in the messages you send.
- Depending on who might have physical access to your computer, clearing email-related traces from your temporary files might be just as important as protecting your messages as they travel across the Internet. See *Chapter 6: How to destroy sensitive information* and the *CCleaner Guide* for details.

TIPS ON RESPONDING TO SUSPECTED EMAIL SURVEILLANCE

If you suspect that someone is already monitoring your email, you may want to create a new account and keep the old one as a decoy. Remember, though, that any account with which you have exchanged email in the past may now be under surveillance as well. As a result, you should observe some additional precautions:

- Both you and your recent email contacts should create new accounts and connect to them only from locations, such as Internet cafes, that you have never used before. We recommend this strategy in order to prevent connections from your usual computer, which may be monitored, from giving away the location of your new account. As an alternative, if you must login to your new account from your normal location, you can use one of the tools described in *Chapter 8: How to remain anonymous and bypass censorship on the Intenret*, to hide these connections.
- Exchange information about these new email addresses only through secure channels, such as a face-to-face meetings, secure instant messages or encrypted **VoIP** conversations.
- Keep the traffic on your old account mostly unchanged, at least for a while. It should appear to the eavesdropper as if you are still using that account for sensitive communication. Presumably, you will want to avoid revealing critical information, but you should try not to make it obvious that you are doing so. As you can imagine, this may be somewhat challenging.

- Make it difficult to link your actual identity to your new account. Do not send email between the new account and your old accounts (or the accounts of any contacts whom you think may also be monitored).
- Be aware of what you write when using your new account. It is best to avoid using real names and addresses or phrases like 'human rights' or 'torture.' Develop an informal code system with your email contacts and change it periodically.
- Remember, email security is not just about having strong technical defences. It is about paying attention to how you and your email contacts communicate with each other, and about remaining disciplined in your non-technical security habits.

SECURING OTHER INTERNET COMMUNICATION TOOLS

Much like email, instant messaging and **VoIP** software can be secure or insecure, depending on the tools you choose and how you use them.

Securing your instant messaging software

Instant messaging, also called 'chat,' is not normally secure, and can be just as vulnerable to surveillance as email. Luckily, there are programs that can help secure the privacy of your chat sessions. Just like with email, though, a secure communications channel requires that both you and your instant messaging contacts use the same software and take the same security precautions.

There is a chat program called **Pidgin** that supports many existing instant messaging protocols, which means that you can easily begin using it without having to change your account name or recreate your list of contacts. In order to have private, **encrypted** conversations through Pidgin, you will need to install and activate the *Off-the-Record* (**OTR**) plug-in. Fortunately, this is a fairly simple process.

Hands-on: Get started with the *Pidgin Guide*

Skype, which is a common **VoIP** tool, also supports instant messaging. While using Skype is probably more secure than using one of the alternatives without the **OTR** plugin, it has two important drawbacks. First, it only allows you to chat with other Skype users, whereas **Pidgin** can be used to communicate securely with nearly all other instant messaging services. Second, because it is closed-source, it is impossible to verify the strength of its **encryption**. *Chapter 1: How to protect your computer from malware and hackers* addresses the virtues of Free and Open-Source Software (**FOSS**) in the *Keeping your software up-to-date* section. In short, you are better off using Pidgin, with the OTR plugin, for secure instant messaging.

Pablo: ***If Yahoo webmail is insecure, does that mean that Yahoo Chat is insecure, too?***

Claudia: ***The thing to remember is that, if we want to use instant messaging to discuss this report, we need to make sure that everyone involved has Pidgin and OTR installed. If they do, we can use Yahoo chat or any other chat service.***

Securing your VoIP software

VoIP calls to other VoIP users are generally free of charge. Some programs allow you to make inexpensive calls to normal phones as well, including international numbers. Needless to say, these features can be extremely useful. Some of today's more popular VoIP programs include **Skype**, *Gizmo* [1], *Google Talk* [2], *Yahoo! Voice* [3], and *MSN Messenger* [4].

Normally, voice communication over the Internet is no more secure than unprotected email and instant messaging. Only Skype and **Gizmo** offer encryption for voice conversations, and then only if you are calling another VoIP user, as opposed to a mobile or landline telephone. In addition, because neither application is open-source, independent experts have been unable to test them fully and ensure that they are secure.

ADVANCED EMAIL SECURITY

The tools and concepts discussed below are recommended for experienced computer users.

Using public key encryption in email

It is possible to achieve a greater level of email privacy, even with a non-secure email account. In order to do this, you will need to learn about public key **encryption**. This technique allows you to encode individual messages, making them unreadable to anyone but the intended recipients. The ingenious aspect of public key encryption is that you don't have to exchange any secret information with your contacts about how you are going to encode messages in the future.

Pablo: *But how does all this work?*
Claudia: ***Clever mathematics! You encode messages to a given email***

contact using her special 'public key,' which she can distribute freely. Then, she uses her secret 'private key,' which she has to guard carefully, in order to read those messages. In turn, your contact uses your public key to encrypt messages that she writes to you. So, in the end, you do have to exchange public keys, but you can share them openly, without having to worry about the fact that anybody who wants your public key can get it.

This technique can be used with any email service, even one that lacks a secure communication channel, because individual messages are **encrypted** before they leave your computer.

Remember that, by using encryption, you could attract attention to yourself. The type of encryption used when you access a secure website, including a webmail account, is often viewed with less suspicion than the type of public key encryption being discussed here. In some circumstances, if an email containing this sort of encrypted data is intercepted or posted to a public forum, it could incriminate the person who sent it, regardless of the message's content. You might sometimes have to choose between the privacy of your message and the need to remain inconspicuous.

Encrypting and authenticating individual messages

Public key encryption may seem complicated at first, but it is quite straightforward once you understand the basics, and the tools are not difficult to use. The Mozilla **Thunderbird** email program can be used with an extension called **Enigmail** to encrypt and decrypt email messages quite easily.

Hands-on: Get started with the *Thunderbird Guide*

VaultletSuite 2 Go, a freeware encrypted email program, is even easier to use than Thunderbird if you are willing to trust the company that provides it and allow them to do some of the work for you.

Hands-on: Get started with the *VaultletSuite 2Go Guide*

The authenticity of your email is another important aspect of communication security. Anyone with Internet access and the right tools can impersonate you by sending messages from a fake email address that is identical to your own. The danger here is more apparent when considered from the perspective of the recipient. Imagine, for example, the threat posed by an email that appears to be from a trusted contact but is actually from someone whose goal is to disrupt your activities or learn sensitive information about your organisation.

Because we cannot see or hear our correspondents through email, we typically rely on a sender's address to verify her identity, which is why we are so easily fooled by fake emails. **Digital signatures**, which also rely on public key **encryption**, provide a more secure means of proving one's identity when sending a message. The *How to use Enigmail with Thunderbird* section of the *Thunderbird Guide* explains in detail how this is done.

Pablo: *I had a colleague once who received email from me that I didn't send. We decided, in the end, that it was just spam, but now I'm imagining how much damage could be done if a fake email appeared in the wrong person's inbox at the wrong time. I've heard you can prevent this kind of thing with digital signatures, but what are they?*

Claudia: *A digital signature is like a wax seal over the flap of an envelope with your letter inside. Except that It can't be forged. It proves that you are the real sender of the message and that it hasn't been tampered with along the way.*

FURTHER READING

- To learn more about faking an email identity, refer to the *Spoofing* section of the *Digital Security and Privacy for Human Rights Defenders* book [5].
- There is a well-known *Man in the Middle attack* [5] attack on SSL encryptionas discussed in the *Digital Security and Privacy for Human Rights Defenders* book.
- The *Gmail Privacy Policy* [6], which you must accept when creating a Gmail account, explains that, "Google maintains and processes your Gmail account and its contents to provide the Gmail service to you and to improve our services." In fact, all email providers scan your messages, to some extent, so that they can offer anti-spam services and other such features. Gmail goes a bit futher, however, in order to provide 'targeted advertising' based on the actual content of your email. This could be dangerous if information stored by Google were to be intentionally or accidentally exposed.
- A series of interviews in 2008 addressed the *privacy and encryption policies* [7] of several major instant messaging services.
- In addition to the *RiseUp* and *Thunderbird* Hands-on Guides, there

are a number of websites that explain how to use your email program with various popular email providers while leaving a copy of your messages on the mail server:

- The *Riseup* [8] website
- Instructions on using *Gmail* [9]
- Instructions on *how to import your gmail contacts into Thunderbird* [10]
- For details on how to use other email services in this way, search the help section of the provider's website for keywords like 'POP', 'IMAP' and 'SMTP'.

LINKS

[1] ***www.gizmo5.com/pc***
[2] ***www.google.com/talk***
[3] ***www.voice.yahoo.com***
[4] ***www.download.live.com/?sku=messenger***
[5] ***www.frontlinedefenders.org/manual/en/esecman***
[6] ***https://mail.google.com/mail/help/intl/en/privacy.html***
[7] ***www.news.cnet.com/8301-13578_3-9962106-38.html***
[8] ***http://help.riseup.net/mail/mail-clients***
[9] ***https://mail.google.com/support/bin/topic.py?topic=12805***
[10] ***www.email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm***

8
How to remain anonymous and bypass censorship on the Internet

8. How to remain anonymous and bypass censorship on the Internet

Many countries around the world have installed software that prevents Internet users within those countries from accessing certain websites and Internet services. Companies, schools and public libraries often use similar software to protect their employees, students and patrons from material that they consider distracting or harmful. This kind of filtering technology comes in a number of different forms. Some filters block a site based on its **IP address**, while others blacklist certain **domain names** or search through all unencrypted Internet communication, looking for specific keywords.

Regardless of what filtering methods are present, it is nearly always possible to evade them by relying on intermediary computers, outside your country, to reach blocked services for you. This process is often called censorship circumvention, or simply **circumvention**, and the intermediary computers are called **proxies**. Proxies, too, come in many different forms. This chapter includes a brief discussion of multiple-proxy anonymity networks followed by a more thorough description of basic **circumvention proxies** and how they work.

Both of these methods are effective ways to evade Internet filters, although the former is most appropriate if you are willing to sacrifice speed in order to keep your Internet activities as anonymous as possible. If you know and trust the individual or organization that operates your proxy, or if performance is more important to you than anonymity, then a basic circumvention proxy might serve you better.

Background scenario

Mansour and Magda are siblings, in an Arabic-speaking country, who maintain a blog on which they anonymously publicise human rights abuses and campaign for political change. The authorities in their country have not been able to shut down their website, because it is hosted in another country, but they have often tried to learn the identity of the blog's administrators from other activists. Mansour and Magda are concerned that the authorities may be able to monitor their updates and learn who they are. In addition, they want to prepare for when the government eventually filters their website, not only so that they can continue updating it, but also in order to provide good circumvention advice to readers within

their own country, who would otherwise lose access to the blog.

What you can learn from this chapter

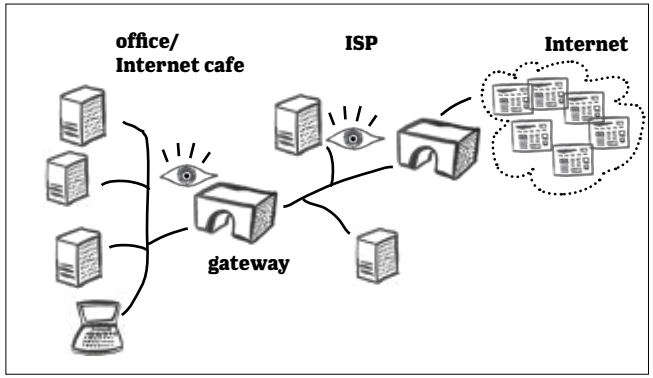
- How to access a website that is blocked from within your country
- How to prevent websites that you visit from knowing your location
- How to ensure that neither your **ISP** nor a surveillance organization in your country can determine which websites and Internet services you visit

UNDERSTANDING INTERNET CENSORSHIP

Research carried out by organisations like the *OpenNet Initiative (ONI)* [1] and *Reporters Without Borders (RSF)* [2] indicates that many countries filter a wide variety of social, political and 'national security' content, while rarely publishing precise lists of what has been blocked. Naturally, those who wish to control their citizens' access to the Internet also make a special effort to block known proxies and websites that offer tools and instruction to help people circumvent these filters.

Despite the guarantee of free access to information enshrined in Article 19 of the Universal Declaration of Human Rights, the number of countries engaged in Internet censorship has continued to increase dramatically over the past few years. As the practice of Internet filtering spreads throughout the world, however, so does access to the circumvention tools that have been created, deployed and publicised by activists, programmers and volunteers.

Before exploring the various ways to bypass Internet censorship, you should first develop a basic understanding of how these filters work. In doing so, it may be helpful to consider a greatly-simplified model of your connection to the Internet.



Your Internet connection

The first step of your connection to the Internet is typically made through an ***Internet Service Provider*** (**ISP**) at your home, office, school, library or Internet cafe. The ISP assigns your computer an **IP address**, which various Internet services can use to identify you and send you information, such as the emails and webpages you request. Anyone who learns your IP address can figure out what city you are in. Certain well-connected organisations in your country, however, can use this information to determine your precise location.

- **Your ISP** will know which building you are in or which phone line you are using if you access the Internet through a modem.
- **Your Internet cafe, library or business** will know which computer you were using at a given time, as well as which port or wireless access point you were conncted to.
- **Government agencies** may know all of these details, as a result of their influence over the organisations above.

At this stage, your **ISP** relies on the network infrastructure in your country to connect its users, including you, with the rest of the world. On the other end of your connection, the website or Internet service you are accessing has gone through a similar process, having received its own IP addresses from an ISP in its own country. Even without all of the technical details, a basic model like this can be helpful when considering the various tools that allow you get around filters and remain anonymous on the Internet.

How websites are blocked

Essentially, when you go to view a webpage, you are showing the site's **IP address** to your **ISP** and asking it to connect you with the webserver's ISP. And, if you have an unfiltered Internet connection, it will do precisely that. If you are in a country that censors the Internet, however, it will first consult a **blacklist** of forbidden websites and then decide whether or not to comply with your request.

In some cases, there may be a central organisation that handles filtering in place of the **ISPs** themselves. Often, a blacklist will contain **domain names**, such as www.blogger.com, rather than **IP addresses**. And, in some countries, filtering software monitors your connection, rather than trying to block specific Internet addresses. This type of software scans through the requests that you make and the pages that are returned to you, looking for sensitive key words and then deciding whether or not to let you see the results.

And, to make matters worse, when a webpage is blocked you may not even know it. While some filters provide a 'block page' that explains why a particular page has been censored, others display misleading error messages. These messages may imply that the page cannot be found, for example, or that the address was misspelled.

In general, it is easiest to adopt a worst-case perspective toward Internet censorship, rather than trying to research all of the particular strengths and weaknesses of the filtering technologies used in your country. In other words, you might as well assume that:

- Your Internet traffic is monitored for keywords
- Filtering is implemented directly at the **ISP** level
- Blocked sites are **blacklisted** by both their **IP addresses** and their **domain names**
- You may be given an unclear or misleading reason to explain why a blocked site fails to load.

Because the most effective circumvention tools can be used regardless of which filtering methods are in place, it does not generally do any harm to make these pessimistic assumptions

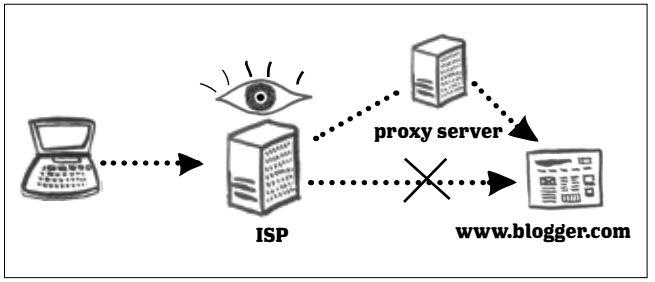
Mansour: *So, if I find one day that I can't access the blog, but a friend in another country can still see it just fine, does that mean the government has blocked it?*

Magda: *Not necessarily. There could be some problem that only affects people who are trying to reach the website from here. Or, it could be some issue with your computer that only shows up on certain types of webpages. You're on the right track, though. You could also try visiting it yourself while using a circumvention tool. After all, most of these tools rely on external proxy servers, which is a bit like asking a friend in another country to test a website for you, except you get to do it yourself.*

UNDERSTANDING CENSORSHIP CIRCUMVENTION

If you cannot go prodirectly to a website because it is blocked by one of the methods discussed above, you will need to find a way around the obstruction. A secure **proxy** server, located in a country that does not filter the Internet, can provide this kind of detour by fetching the webpages you request and delivering them to you. From your **ISP**'s perspective, you will simply appear to be communicating securely with an unknown computer (the proxy server) somewhere on the Internet.

Of course, the government agency in charge of Internet censorship in your country (or the company that provides updates for its filtering software) might eventually learn that this 'unknown computer' is really



a circumvention proxy. If that happens, its **IP address** may itself be added to the blacklist, and it will no longer work. It usually takes some time for proxies to be blocked, however, and those who create and update circumvention tools are well aware of this threat. They typically fight back using one or both of the following methods:

- **Hidden proxies** are more difficult to identify. This is one of the reasons why it is important to use secure proxies, which tend to be less obvious. **Encryption** is only part of the solution, however. The operators of a proxy must also take care when revealing its location to new users if they want it to remain hidden.
- **Disposable proxies** can be replaced very quickly after they are blocked. In this case, the process of telling users how to find replacement proxies may not be particularly secure. Instead, circumvention tools of this type often simply try to distribute new proxies faster than they can be blocked.

In the end, as long as you can reach a **proxy** that you trust to fetch the services you ask for, all you have to do is send it your requests and view whatever comes back using the appropriate Internet application. Typically, the details of this process are handled automatically by circumvention software that you install on your computer, by modifying your browser settings or by pointing your browser to a web-based proxy page. The **Tor** anonymity network, described below, uses the first method. Following that is a discussion of basic, single-proxy circumvention tools, each of which works in a slightly different manner.

ANONYMITY NETWORKS AND BASIC PROXY SERVERS

Anonymity networks

Anonymity networks typically 'bounce' your Internet traffic around between various secure **proxies** in order to disguise where you are coming from and what you are trying to access. This can significantly

reduce the speed at which you are able to load websites and other Internet services. In the case of Tor, however, it also provides a reliable, secure and public means of circumvention that saves you from having to worry about whether or not you trust the individuals who operate your proxies and the websites you visit. As always, you must ensure that you have an encrypted connection, using **HTTPS**, to a secure website before exchanging sensitive information, such as passwords and emails, through a browser.

You will have to install software to use **Tor**, but the result is a tool that provides anonymity as well as circumvention. Each time you connect to the Tor network, you select a random path through three secure **Tor proxies**. This ensures that neither your ISP nor the proxies themselves know both your computer's **IP address** and the location of the Internet services you request. You can learn much more about this tool from the Tor Guide.

Hands-on: Get started with the *Tor Guide*

One of Tor's strengths is that it does not just work with a browser but can be used with various types of Internet software. Email programs, including Mozilla **Thunderbird**, and instant messaging programs, including **Pidgin**, can operate through Tor, either to access filtered services or to hide your use of those services.

Basic circumvention proxies

There are three important questions that you should consider when selecting a basic circumvention **proxy**. First, is it a web-based tool or does it require you to change settings or install software on your computer? Second, is it secure? Third, is it private or public?

Web-based and other proxies:

Web-based **proxies** are probably the easiest to use. They require only that you point your browser at a proxy webpage, enter the filtered address you wish to view and click one button. The proxy will then display the requested content inside its own webpage. You can follow links normally or enter a new address into the proxy if you want to view a different page. You do not need to install any software or change any browser settings, which means that web-based proxies are:

- Easy to use
- Reachable from public computers, such as those at Internet cafes, that may not allow you to install programs or change settings
- Potentially safer if you are concerned about being 'caught' with circumvention software on your computer

Web-based proxies tend to have certain disadvantages, as well. They do not always display pages correctly, and many web-based proxies will fail to load complex websites, including those that feature streaming audio and video content. Also, while any proxy will slow down as it gains more users, this tends to be more of an issue with public web-based proxies. And, of course, web-based proxies only work for webpages. You can not, for example, use an instant messaging program or an email client to access blocked services through a web-based proxy. Finally, secure web-based proxies offer limited confidentiality because they must themselves access and modify the information returned to you by the websites you visit. If they did not, you would be unable to click on a link without leaving the proxy behind and attempting to make a direct connection to the target webpage. This is discussed further in the following section.

Other types of proxies generally require you to install a program or configure an external proxy address in your browser or operating system. In the first case, your circumvention program will typically provide some way of turning the tool on and off, which will tell your browser whether or not to use the proxy. Software like this often allows you to change proxies automatically if one is blocked, as discussed above. If you have to configure an external proxy address in your browser or operating system, you will need to learn the correct proxy address, which may change if that proxy is blocked or slows down so much that it becomes unusable.

Although it may be slightly more difficult to use than a web-based proxy, this method of circumvention is more likely to display complex pages correctly and may take longer to slow down as more people begin to use a given proxy server. Furthermore, proxies can be found for a number of different Internet applications. Examples include HTTP proxies for browsers, SOCKS proxies for email and chat programs and VPN proxies, which can redirect all of your Internet traffic to avoid filtering.

Secure and insecure proxies:

A secure proxy, in this chapter, refers to any **proxy** that supports **encrypted** connections from its users. An insecure proxy will still allow you to bypass many types of filtering, but will fail if your Internet connection is being scanned for key words or particular website addresses. It is a particularly bad idea to use an insecure proxy when accessing websites that are normally encrypted, such as webmail accounts and banking websites. By doing so, you may expose sensitive information that would normally be hidden. And, as mentioned previously, insecure

proxies are often easier for those who update Internet filtering software and policies to discover and block. In the end, the fact that free, fast, secure proxies exist means that there are very few good reasons to settle for an insecure one.

You will know that a web-based proxy is secure if you can access the proxy webpage itself using an **HTTPS** address. As with webmail services, secure and insecure connections may be supported, so you should be certain to use the secure address. Often, in such cases, you will have to accept a 'security certificate warning' from your browser in order to continue. This is the case for both the **Psiphon** and **Peacefire** proxies, discussed below. Warnings like this tell you that someone, such as your ISP or a hacker, could be monitoring your connection to the proxy. Despite these warnings, it is still a good idea to use secure proxies whenever possible. However, when relying on such proxies for circumvention, you should avoid visiting secure websites, entering passwords or exchanging sensitive information unless you verify the proxy's SSL fingerprint. In order to do this, you will need a way of communicating with the proxy's administrator.

Appendix C of the *Psiphon User's Guide* [3] explains the steps that both you and the proxy administrator should follow in order to verify the proxy's fingerprint.

You should also avoid accessing sensitive information through a web-based proxy unless you trust the person who runs it. This applies regardless of whether or not you see a security certificate warning when you visit the proxy. It even applies if you know the proxy operator well enough to verify the server's fingerprint before directing your browser to accept the warning. When you rely on a single proxy server for circumvention, its administrator will always know your IP address and which websites you are accessing. More importantly, however, if that proxy is web-based, a malicious operator could gain access to all of the information that passes between your browser and the websites you visit, including the content of your webmail and your passwords.

For proxies that are not web-based, you may have to do a little research to determine whether or not secure connections are supported. All of the proxies and anonymity networks recommended in this chapter are secure.

Private and public proxies:

Public proxies accept connections from anyone, whereas private **proxies** typically require a username and password. While public proxies have the obvious advantage of being freely available, assuming they can be found, they tend to become overcrowded very quickly. As a result, even though public proxies may be as technically sophisticated and well-maintained as private ones, they are often relatively slow. Finally, private proxies tend to be run either as for-profit businesses or by administrators who create accounts for users that they know personally or socially. Because of this, it is generally easier to determine what motivates the operators of a private proxy. You should not assume, however, that private proxies are therefore fundamentally more trustworthy. After all, the profit motive has led online services to expose their users in the past.

Simple, insecure, public proxies can often be found by searching for terms like 'public proxy' in a search engine, but you should not rely on proxies discovered this way. Given the choice, it is better to use a private, secure proxy run by people that you know and trust, either personally or by reputation, and who have the technical skill to keep their server secure. Whether or not you use a web-based proxy will depend on your own particular needs and preferences. Any time you are using a proxy for circumvention, it is also a good idea to use the **Firefox** browser and to install the NoScript browser extension, as discussed in the *Firefox Guide*. Doing so can help protect you both from malicious **proxies** and from websites that might try to discover your real **IP address**. Finally, keep in mind that even an encrypted proxy will not make an insecure website secure. You must still ensure that you have an **HTTPS** connection before sending or receiving sensitive information.

If you are unable to find an individual, organisation or company whose proxy service you consider trustworthy, affordable and accessible from your country, you should consider using the Tor anonymity network, which is discussed above, under *Anonymity networks*.

SPECIFIC CIRCUMVENTION PROXIES

Below are a few specific tools and proxies that can help you circumvent Internet filtering. New circumvention tools are produced regularly, and existing ones are updated frequently, so you should visit the online Security in-a-Box website, and the resources mentioned in the *Further reading* section below, to learn more.

Sesawe Hotspot Shield is a public, secure, non-web-based, freeware circumvention proxy. In order to use it, you will need to *download the tool* [4] and install it. The company that develops Hotspot Shield receives funding from advertisers, so you will see a 'banner ad' at the top of your browser window whenever you use it to visit websites that do not provide **encryption**. Although it is impossible to verify, this company claims to delete the **IP addresses** of those who use the tool, rather than storing or sending them to advertisers. Because Hotspot

Shield relies on a Virtual Private Network (VPN), your entire Internet connection will pass through the proxy while you are 'connected'. This can be helpful if you use email or instant messaging providers that are filtered in your country. You can learn more about Hotspot Shield from *AnchorFree website* [5].

Psiphon may be a good option if you know someone who has a Windows computer that she leaves on, running and connected to a fast, unfiltered Internet connection in another country. In order to use **Psiphon**, you must ask this person to download the program from the *Psiphon website* [6], install it, create an account for you, and send you the proxy's IP address along with your username and password. This will give you access to your own personal account on a trusted, secure, private, web-based circumvention proxy. Before using it, however, you should verify the proxy's fingerprint as discussed in the *Secure and insecure proxies* section, above, and in *Appendix C* of the included *Psiphon User's Guide* [3].

Your-Freedom is a private, secure, non-web-based circumvention **proxy**. It is a **freeware** tool that that can be used to access a free circumvention service. You can also pay a fee to access a commercial service, which is faster and has fewer limitations. In order to use *Your-Freedom*, you will need to *download the tool* [7] and *create an account* [8], both of which can be done at the *Your-Freedom website* [9]. You will also need to configure your browser to use the proxy when connecting to the Internet. You can learn how to do this from the *Sesawe Project website* [10].

Peacefire maintains a large number of public, web-based proxies, which can be secure or insecure, depending on how you access them. When using a Peacefire proxy, you must enter the HTTPS address in order to have a secure connection between yourself and the proxy. New proxies are announced to a large mailing list on a regular basis. You can sign up to receive updates at the *Peacefire website* [11].

Mansour: ***Great! So our ISP can't see what we're doing when I use a proxy server, right?***

Magda: ***As long as we use a secure proxy, and give some thought to any 'security certificate warnings' that might pop up, then yes. That's true. Keep in mind that an insecure proxy will still let you get around most Internet filters, but it will also let your ISP snoop on your connection, including the location of the pages you're visiting.***

FURTHER READING

- See the *Internet Surveillance and Monitoring* and *Censorship circumvention* chapters of the *Digital Security and Privacy Manual for Human Rights Defenders* book [12].
- The FLOSS Manuals website contains a guide on *How to Bypass Internet Censorship* [13].
- The *Sesawe Project's website* [14] maintains a list of circumvention tools and other information about Internet filtering.
- The *Internet Censorship Wiki* [15], written by Freerk, is available in English, German and Spanish.
- The CitizenLab has produced *Everyone's guide to by-passing Internet Censorship* [16], which is being translated into Burmese, English, French, Russian, Spanish and Urdu.
- Reporters Without Borders has released a second edition of its *Handbook for Bloggers and Cyberdissidents* [17], which is available in Arabic, Burmese, Chinese, English, Farsi, French, Russian and Spanish.
- Ethan Zuckerman of Global Voices Online has published a useful guide to *Anonymous Blogging with Wordpress and Tor* [18].

LINKS

[1] ***www.opennet.net***
[2] ***www.rsf.org***
[3] ***www.psiphon.ca/guides.html***
[4] ***https://sesawe.net/Anchor-Free-Hotspot-Shield.html***
[5] ***www.hotspotshield.com***
[6] ***www.psiphon.ca***
[7] ***www.your-freedom.net/index.php?id=3***
[8] ***www.your-freedom.net/index.php?id=170***
[9] ***www.your-freedom.net*** [6] ***www.psiphon.ca/guides.html***
[10] ***https://sesawe.net/Using-Your-Freedom.html***
[11] ***www.peacefire.org***
[12] ***www.frontlinedefenders.org/manual/en/esecman/***
[13] ***www.flossmanuals.net/CircumventionTools***
[14] ***https://sesawe.net/***
[15] ***www.en.cship.org/wiki/Main_Page***
[16] ***www.civisec.org/sites/all/themes/civisec/guides/everyone%27s-guide-english.pdf***
[17] ***www.rsf.org/rubrique.php3?id_rubrique=542***
[18] ***http://advocacy.globalvoicesonline.org/tools/guide***

Glossary

Glossary

Some of the technical terms that you will encounter as you read through these chapters are defined below:

Avast - A freeware anti-virus tool
BIOS (Basic Input/Output System) - The first and deepest level of software on a computer. The BIOS allows you to set many advanced preferences related to the computer's hardware, including a start-up password
Blacklist - A list of blocked websites and other Internet services that can not be accessed due to a restrictive filtering policy
Booting - The act of starting up a computer
CCleaner - A freeware tool that removes temporary files and potentially sensitive traces left on your hard drive by programs that you have used recently and by the Windows operating system itself
CD Burner - A computer CD-ROM drive that can write data on blank CDs. DVD burners can do the same with blank DVDs. CD-RW and DVD-RW drives can delete and rewrite information more than once on the same CD or DVD.
Circumvention - The act of bypassing Internet filters to access blocked websites and other Internet services
Clam Win - A FOSS Anti-virus program for Windows
Cobian Backup - A FOSS backup tool. At any given time, the most recent version of Cobian is closed-source freeware, but prior versions are released as FOSS.
Comodo Firewall - A freeware firewall tool
Cookie - A small file, saved on your computer by your browser, that can be used to store information for, or identify you to, a particular website
Digital signature - A way of using encryption to prove that a particular file or message was truly sent by the person who claims to have sent it
Domain name - The address, in words, of a website or Internet service; for example: security.ngoinabox.org
Encryption - A way of using clever mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key
Enigmail - An add-on for the Thunderbird email program that allows it to send and receive encrypted and digitally signed email
Eraser - A tool that securely and permanently deletes information from your computer or removable storage device

Firefox - A popular FOSS Web browser that provides an alternative to Microsoft Internet Explorer

Firewall - A tool that protects your computer from untrusted connections to or from local networks and the Internet

FOSS (Free and Open Source Software) - This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it

Freeware - Includes software that is free of charge but subject to legal or technical restrictions that prevent users from accessing the source code used to create it

GNU/Linux - A FOSS operating system that provides an alternative to Microsoft Windows

Hacker - In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely

HTTPS - When you are connected to a website through SSL, the address of the website will begin with HTTPS rather than HTTP.

IP address (Internet Protocol address) – A unique identifier assigned to your computer when it is connected to the Internet

ISP (Internet Service Provider) - The company or organisation that provides your initial link to the Internet. The governments of many countries exert control over the Internet, using means such as filtering and surveillance, through the ISPs that operate in those countries.

Keylogger - A type of spyware that records which keys you have typed on your computer's keyboard and sends this information to a third party. Keyloggers are frequently used to steal email and other passwords.

KeePass - A freeware secure password database

LiveCD - A CD that allows your computer to run a different operating system temporarily.

Malware - A general term for all malicious software, including viruses, spyware, trojans, and other such threats

Mnemonic device - A simple trick that can help you remember complex passwords

NoScript - A security add-on for the Firefox browser that protects you from malicious programs that might be present in unfamiliar webpages

OTR (Off the Record) - An encryption plugin for the Pidgin instant messaging program

Peacefire - Subscribers to this free service receive periodical emails containing an updated list of circumvention proxies, which can be used to bypass Internet censorship

Physical threat - In this context, any threat to your sensitive information that results from other people having direct physical access your computer hardware or from other physical risks, such as breakage, accidents or natural disasters

Pidgin - A FOSS instant messaging tool that supports an encryption plugin called Off the Record (OTR)

Proxy - An intermediary service through which you can channel some or all of your Internet communication and that can be used to bypass Internet censorship. A proxy may be public, or you may need to log in with a username and password to access it. Only some proxies are secure, which means that they use encryption to protect the privacy of the information that passes between your computer and the Internet services to which you connect through the proxy.

Proprietary software - The opposite of Free and Open-Source Software (FOSS). These applications are usually commercial, but can also be freeware with restrictive license requirements.

Riseup - An email service run by and for activists that can be accessed securely either through webmail or using an email client such as Mozilla Thunderbird

Router - A piece of networking equipment through which computers connect to their local networks and through which various local networks access the Internet. Switches, gateways and hubs perform similar tasks, as do wireless access points for computers that are properly equipped to use them

Secure password database - A tool that can encrypt and store your passwords using a single master password

SSL (Secure Sockets Layer) – The technology that permits you to maintain a secure, encrypted connection between your computer and some of the websites and Internet services that you visit.

Security certificate - A way for secure websites and other Internet services to prove, using encryption, that they are who they claim to be. In order for your browser to accept a security certificate as valid, however, the service must pay for a digital signature from a trusted organization. Because this costs money that some service operators are unwilling or unable to spend, however, you will occasionally see a security certificate error even when visiting a valid service.

Security policy - A written document that describes how your organization can best protect itself from various threats, including a list of steps to be taken should certain security-related events take place

Security cable - A locking cable that can be used to secure a laptop or other piece of hardware, including external hard drives and some desktop computers, to a wall or a desk in order to prevent it from being physically removed

Server - A computer that remains on and connected to the Internet in order to provide some service, such as hosting a webpage or sending and receiving email, to other computers

SIM card - A small, removable card that can be inserted into a mobile phone in order to provide service with a particular mobile phone company. SIM cards can also store phone numbers and text messages.

Skype - A freeware Voice over IP (VoIP) tool that allows you to speak with other Skype users for free and to call telephones for a fee. The company that maintains Skype claims that conversations with other Skype users are encrypted. Because it is a closed-source tool, there is no way to verify this claim. ***www.skype.com***

Source code - The underlying code, written by computer programmers, that allows software to be created. The source code for a given tool will reveal how it works and whether it may be insecure or malicious.

Spybot - A freeware anti-malware tool that scans for, removes and helps protect your computer from spyware

Steganography - Any method of disguising sensitive information so that it appears to be something else, in order to avoid drawing unwanted attention to it

Swap file - A file on your computer to which information, some of which may be sensitive, is occasionally saved in order to improve performance

Thunderbird - A FOSS email program with a number of security features, including support for the Enigmail encryption add-on

Tor - An anonymity tool that allows you to bypass Internet censorship and hide the websites and Internet services you vist from anyone who may be monitoring your Internet connection, while also disguising your own location from those websites

TrueCrypt - A FOSS file encryption tool that allows you to store sensitive information securely

Undelete Plus - A freeware tool that can sometimes restore information that you may have deleted accidentally

Uninterruptable Power Supply (UPS) - A piece of equipment that allows your critical computing hardware to continue operating, or to shut down gracefully, in the event of a brief loss of power

VautletSuite 2 Go - A Freeware encrypted email program

Voice over IP (VoIP) – The technology that allows you to use the Internet for voice communication with other VoIP users and telephones

Whitelist - A list of websites or Internet services to which some form of access is permitted, when other sites are automatically blocked

Wiping - The process of deleting information securely and permanently

Your-Freedom - A freeware circumvention tool that allows you to bypass filtering by connecting to the Internet through a private proxy. If Your-Freedom is configured properly, your connection to these proxies will be encrypted in order to protect the privacy of your communication.

DISCLAIMER

Software and documentation in this collection of "NGO in a Box - Security Edition" is provided "as is" and we exclude and expressly disclaim all express and implied warranties or conditions of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose so far as such disclaimer is permitted. In no event shall Front Line Tactical Technology Collective or any agent or representatives thereof be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption), however caused under any theory of liability, arising in any way out of the use of or inability to make use of this software, even if advised of the possibility of such damage. Nothing in this disclaimer affects your statutory rights.